TLDR

: We suggest a way to significantly speed up powers-of-tau ceremonies by allowing multiple online participants to simultaneously make contributions.

Context

Powers-of-tau ceremonies are the trust backbone for pairing-based proof schemes, especially universal schemes that rely on polynomial commitments. Despite the universal and updatable nature of powers-of-tau ceremonies, in practice, there is a need to conduct many different ceremonies. Reasons include:

- curve diversity

—The set of pairing-friendly curves used by applications keeps growing. Curves of interest include BN254, BLS12-381, the MNT4/MNT6 pair, as well as BLS12-377 and various curves built using the Cocks-Pinch method.

- size diversity

—Different applications have varying powers of tau size requirements, i.e. require monomials of different sizes. Unfortunately Cheon's attack reduces the security of larger setups and may prevent the emergence of a large one-size-fits-all.

- flavour diversity

—There are various "flavours" of powers-of-tau ceremonies. For example, some applications need only a small number of G2 elements (possibly just one element) whereas other applications require a linear number (e.g. in the size of the target circuit) of both G1 and G2 elements. Some applications (such as Sonic) require some powers of \tau

to be missing. Other applications require auxiliary secrets (often referred to as \alpha

, \beta

, etc.) to be embedded in the setup in addition to the "main" secret \tau

. Any extra element may be exploitable similarly to Cheon's attack, further disincentivising a one-size-fits-all approach.

Construction

Aztec recently pushed forward the state of the art for theirIgnition ceremony, leading to a record-breaking 176 participants in 30 days. Their contribution included queuing online participants as well as streaming the powers of tau into small chunks. The streaming process allowed for participants to download, process, and reupload the powers of tau in 5% chunks.

When a participant was active in Aztec's Ignition all queued participants were waiting idle. We suggest instead immediately passing every processed chunk from one participant to the next to create a pipeline with multiple online participants working in parallel. For example if 5% chunks are used the pipeline would be at most 20 participants deep. Such a pipeline would be "optimistic" because if a participant in the pipeline goes offline or misbehaves the pipeline from that point onwards is discarded and rebuilt.

Optimistic pipelining is a strict scalability improvement. Indeed, an attacker cannot make the ceremony any slower than without pipelining. An attacker can however waste CPU cycles and bandwidth of others, a small cost to pay when the precious resource is trust in the ceremony and human time.

To maximise the benefits of optimistic pipelining one can place the most reliable and fastest participants near the front of the queue, and the least trusted and slowest participants near the back. Prior to participation, one could also do bandwidth and CPU checks to filter out weak participants. Optimistic pipelining does not exclude traditional "blocking" participation which is appropriate for offline participants (e.g. air-gapped participants).

We observe in past ceremonies that the majority of participants, whether invited or self-selected, have reputation at stake. As such, we expect optimistic pipelining to work well in practice and hope for an order of magnitude speed up. Optimistic pipelining may allow for over 1000 participants in 30 days and could possibly unlock the ability to generate significantly larger setups with powers of tau going up to, say, 2^{32}

.