Threshold Signatures from Group Actions

Here we present a simple summary of the of the relevant material to understand to have an overview and good understanding of the literature of threshold signatures from cryptographic group actions.

For the moment it is out of the scope of this document to provide complete overview, but instead want to guide the reader through the most relevant papers and concepts to understand the current state of the art in this area (clearly these are personal opinions)

We assume the reader is familiar with the basic concepts of threshold signatures and group actions. A brief and crude introduction can be read in this blog post.

For the exposition we follow the slides of the talk given by myself at Lleida. Slides can be found here.

With respect to group actions, we refer to 2020/1188, that provides a systemization of the principal definitions.

Note the potentiality of group actions to construct threshold signatures greatly depends

A first overview o For several reasons,