Group Factorisation for Smaller Signatures from Cryptographic Group Actions

Edoardo Signorini (Telsy - Politecnico di Torino)

Abstract: Cryptographic group actions have gained significant attention in recent years for their application on post-quantum sigma protocols and digital signatures. In NIST's recent additional call for post-quantum signatures, three relevant proposals are based on group actions: LESS, MEDS, and ALTEQ. In this talk, we explores signature optimisations leveraging a group's factorisation. We show that if the group admits a direct product factorisation, the group action can be restricted on a quotient space under the equivalence relation induced by the factorisation. If a special class of representative of the quotient space is efficiently computable via a canonical form, the restricted action is effective and does not incur in security loss. We will discuss the application of these techniques to LESS and MEDS, analysing how they will affect the length of signatures and public keys.