



Norwegian University of  
Science and Technology

# KEY EXCHANGE FROM MONODIAL ACTIONS

**Emil August Hovd Olaisen**

NKS 2025 — October 31, 2025

# Group Action

- ▶ For a group  $G$  and set  $X$  a group action is a function  $G \times X \rightarrow X$  such that  $\forall g, h \in G, \forall x \in X$ :
  1.  $e \cdot x = x$ .
  2.  $(g \cdot h) \cdot x = g \cdot (h \cdot x)$ .
- ▶ We will also in addition assume  $\forall x, y \in X, \exists g \in G$ :

$$g \cdot x = y.$$

# Hard Homogeneous Space

- ▶ A Hard Homogeneous Space [Cou06] is a finite commutative group action for which we have that the following problems are easy:
  1. For any two strings  $g, h \in G$  compute  $g \cdot h, g^{-1}$  and determine if they represent the same group element.
  2. Sample  $g \leftarrow G$
  3. Decide if a random string  $h$  is in the set  $X$ .
  4. Decide if two elements  $x, y \in X$  are equal.
  5. For any  $g \in G, x \in X$  compute  $g \cdot x$ .
  
- ▶ We also need the following two problems to be hard
  1. For  $x, y \in X$  find  $g \in G$  such that  $g \cdot x = y$ .
  2. For  $x \in X$  and  $g \cdot x, h \cdot x$ , compute  $g \cdot h \cdot x$ .

# Key-Exchange from Hard Homogeneous Spaces

- ▶ Suppose Alice and Bob agree on some element  $x \in X$ .
- ▶ Alice and Bob may both sample respective elements  $g, h \leftarrow_{\$} G$  and compute  $g \cdot x, h \cdot x$  and send them to the other party.
- ▶ Alice computes  $g \cdot h \cdot x$ , Bob computes  $h \cdot g \cdot x$ . Due to commutativity these set elements are the same.
- ▶ We may think of the following assumptions
  1. For  $x, y \in X$  find  $g \in G$  such that  $g \cdot x = y$ .
  2. For  $x \in X$  and  $g \cdot x, h \cdot x$ , compute  $g \cdot h \cdot x$ .

- ▶ Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) [CLM<sup>+</sup>18] is a post-quantum key-exchange protocol based on Hard Homogeneous Spaces.
- ▶ The protocol does not actually allow for arbitrary computation of any group elements in its group action.
- ▶ Which of the other features of Hard Homogenous Spaces are not needed for key exchange?

# Tensor-MIKE

- ▶ It is in fact not necessary for the action to be based on a group, as inverses never feature in the key-exchange.
- ▶ Module Isogeny Key Exchange (MIKE) [[Rob24](#)] is a post-quantum key-exchange protocol based on Hard Homogeneous Spaces based on actions from a Commutative Module rather than a Commutative Group.
- ▶ There are many open research questions related to this protocol. One of them being what schemes can be realized with Module actions rather than Group actions.
- ▶ Password Authenticated Key-Exchange is one such example [[AEK+22](#)].

# References

-  Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel.  
Password-authenticated key exchange from group actions.  
In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 699–728, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Cham, Switzerland.
-  Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.  
CSIDH: An efficient post-quantum commutative group action.  
In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Cham, Switzerland.
-  Jean-Marc Couveignes.  
Hard homogeneous spaces.  
Cryptology ePrint Archive, Report 2006/291, 2006.
-  Damien Robert.  
The module action for isogeny based cryptography.  
Cryptology ePrint Archive, Report 2024/1556, 2024.