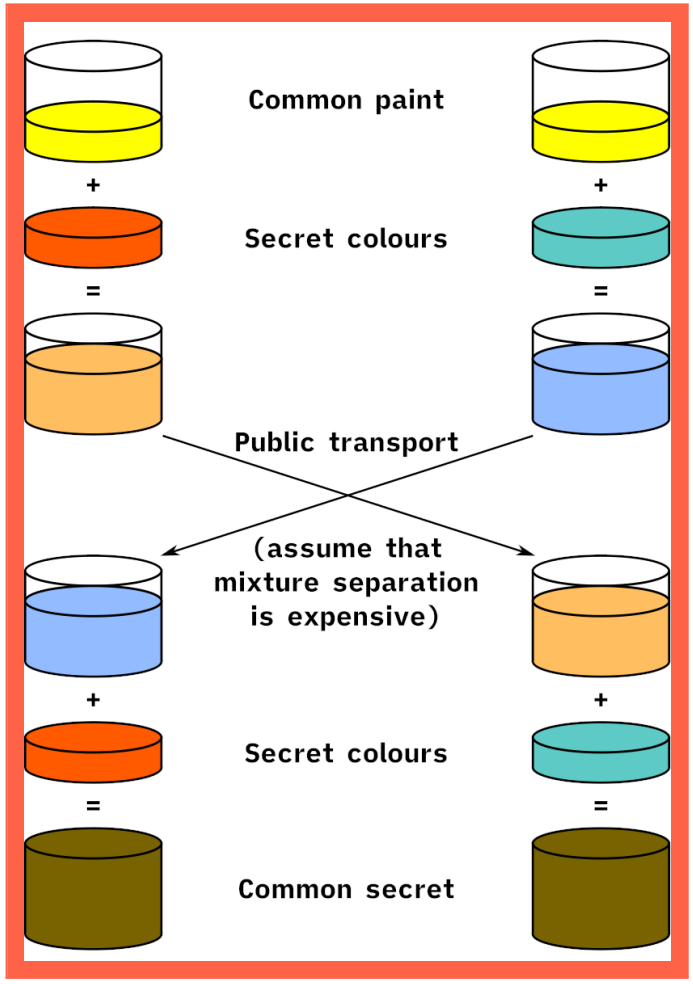
What is...group-based cryptography?

Or: Subfields of mathematics 25

Diffie–Hellman (DH) in action



- DH Two secrets a, b, public g, send mix ag or gb and get agb
- Catch Relies on the mixtures to be hard ot decompose
- BTW Using colors is not very practical ;-)

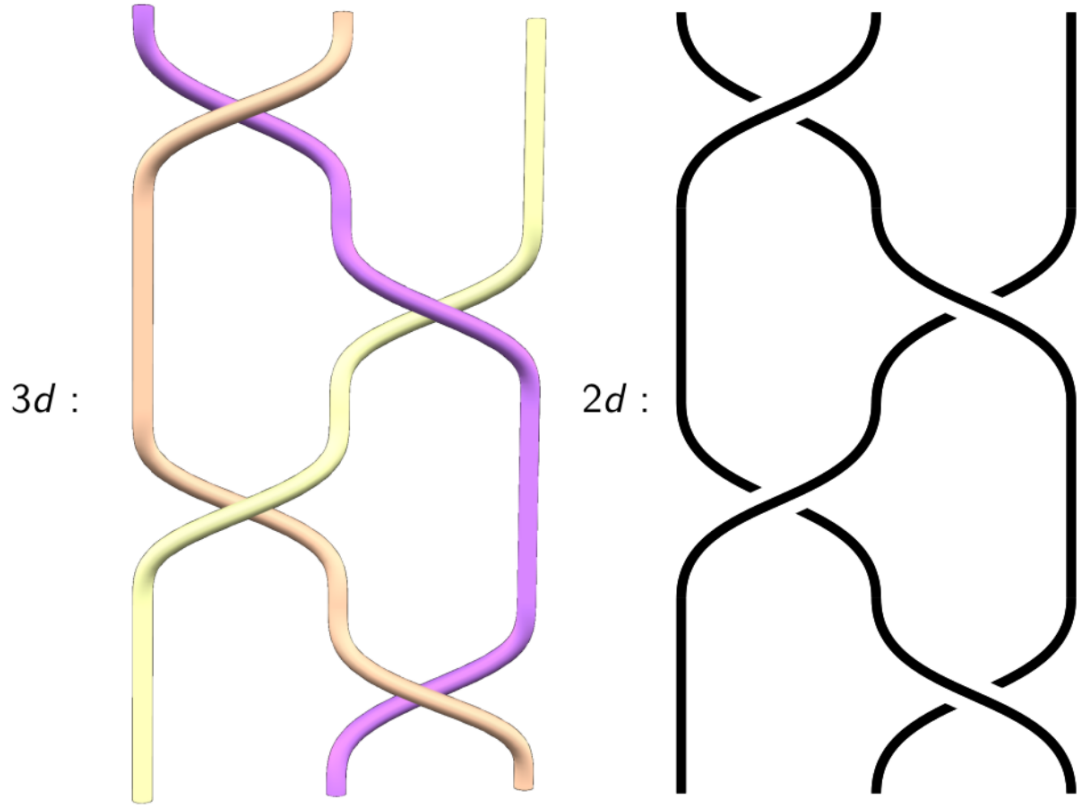
Details

The original DH key exchange:

- Fix $\mathbb{Z}/p\mathbb{Z}$ and $g \in (\mathbb{Z}/p\mathbb{Z})^*$ Public
- Party A fixes $a \in \mathbb{Z}$, party B fixes $b \in \mathbb{Z}$ Private
- Party A sends $g^a \bmod p$, party B sends $g^b \bmod p$ Public
- Party A computes $(g^b \bmod p)^a \bmod p$, party B computes $(g^a \bmod p)^b \bmod p$
  A does not know b and B does not know a
- Common secret $(g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p$

- Theorem/idea Party C knows only p, g, $g^a \bmod p$ and $g^b \bmod p$, and needs to find $g^{ab} \bmod p$; this is the discrete logarithm problem which does not appear to have an efficient algorithm (but there are efficient quantum algorithms)
- Next step? Maybe use a more complicated group $G \neq \mathbb{Z}/p\mathbb{Z}$
- Idea If computations in G are sufficiently complicated, then secrets are safe without relying on 'hacks'

Variation of DH: conjugacy search problem (CSP)

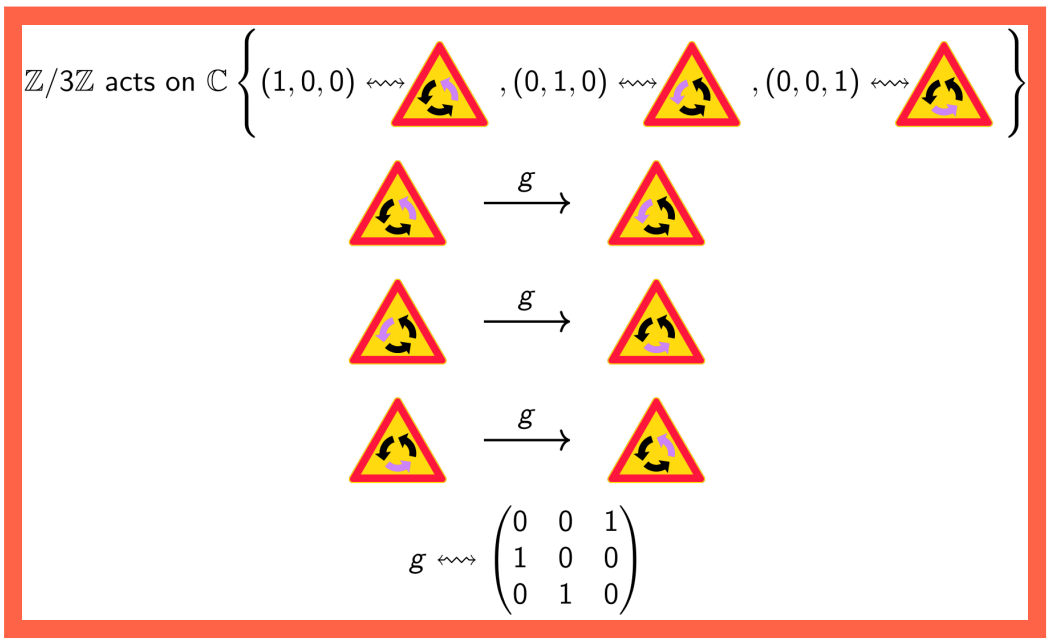


- Group-bases $g^x = xgx^{-1}$ for x in some group G
- Same game, different names $g \in G$ public, $a, b \in G$ private
- Any group G works, but the conjugacy problem should be hard in G
- Proposed candidates include braid groups (albeit these are not optimal)

Enter, the theorem

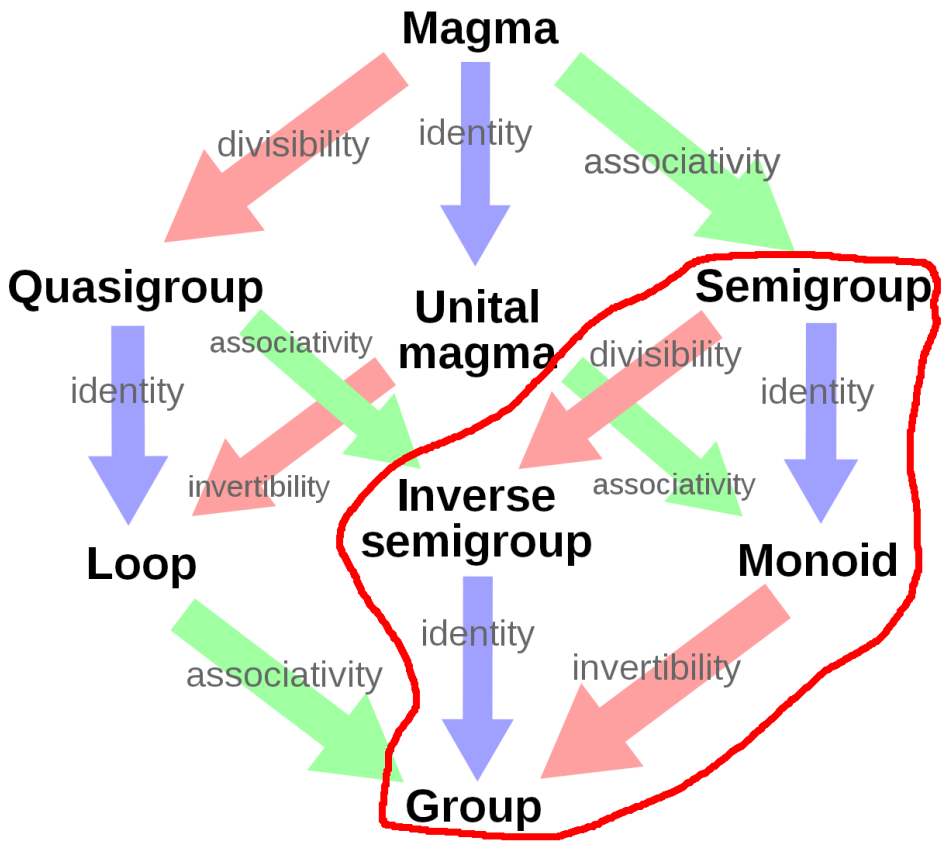
Linear attack If the group G has a nice representation of small dimension, then it is not suited for cryptography without 'hacks' (depends on the used protocol, say the one from the previous slide)

- **Nice** could mean e.g. faithful (=injective); key problem: groups often have small representations
- **Reminder on representations**



- Group-based cryptography answers similar questions!

Linear = bad



- Moral The more linear structure is available the better for party C
- Idea 1 Use monoids/semigroups instead of groups: these tend to have bigger representations than groups
- Idea 2 Work over semirings (like tropicals): these tend to have bigger representations than groups

Thank you for your attention!

I hope that was of some help.