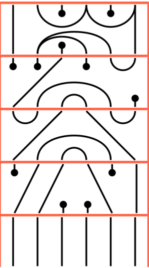
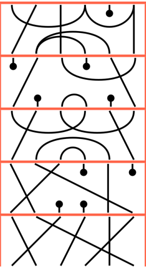
Monoidal categories and cryptography

Or: Monoids in action

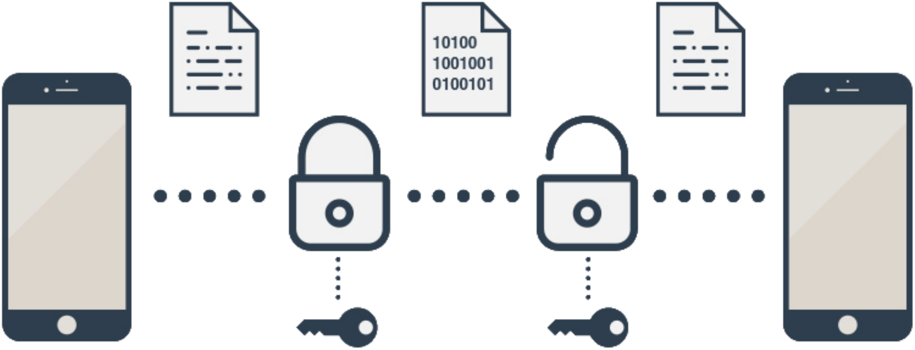
Daniel Tubbenhauer

Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
pPa_n		YES*	Pa_n		YES*
Mo_n		YES	RoBr_n		YES*
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

Joint with Mikhail Khovanov and Maithreya Sitaraman

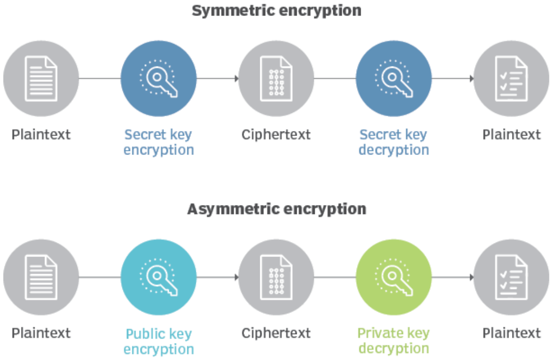
December 2021

End-to-end encryption



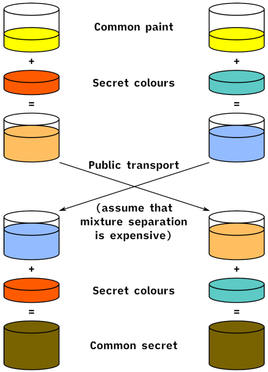
- E2EE Only the two communicating parties should decrypt the message
- Problem How to transfer the encryption key?
- Diffie–Hellman (DH) Addresses this problem

End-to-end encryption



- Symmetric Both parties us the same secret key
- Problem (still) How to transfer the encryption key?
- Asymmetric Both parties have a public and a private key, no sharing needed

End-to-end encryption



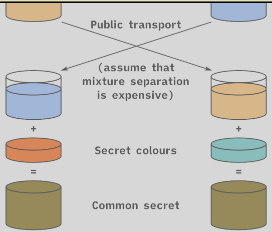
- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^x$

Colors!

The color picture makes it clear that this can easily be generalized

For example, one could take a different group

Varying the protocol and one can even allow arbitrary monoids



- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^x$

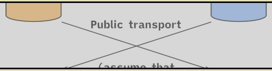
End-to-end encryption

Colors!

The color picture makes it clear that this can easily be generalized

For example, one could take a different group

Varying the protocol and one can even allow arbitrary monoids



Example (Shpilrain–Ushakov (SU) key exchange protocol)

The public data is a monoid S, and two sets $A, B \subset S$ of commuting elements and $g \in S$

Party A chooses privately $a, a' \in A$ and party B chooses privately $b, b' \in A$

Party A communicates aga', B sends bgb' and the common secret is $abgb'a' = baga'b'$

Note that S can be an arbitrary monoid in this protocol

The complexity of S determines how difficult it is to find the common secret from the public data

Linear attack (Myasnikov–Roman'kov ∼2015)

"All" protocol involving monoids can be attacked
if the monoid admits a small non-trivial representation

Enter representation theory

No algebras, please (Myasnikov–Roman'kov ∼2015)

Stay set-theoretical: algebras are easier to attack linearly

- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^{\times}$

Linear attack (Myasnikov–Roman'kov ∼2015)

"All" protocol involving monoids can be attacked
if the monoid admits a small non-trivial representation

Enter representation theory

No algebras, please (Myasnikov–Roman'kov ∼2015)

Stay set-theoretical: algebras are easier to attack linearly

Our idea

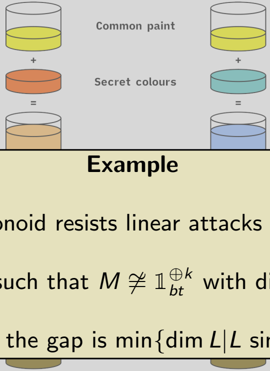
Systematically study and construct monoids with no small non-trivial representations

The abstract theory is governed by Green's theory of cells (Green's relations)

The good finite examples come from quantum topology and monoidal categories

Monoidal categories provide families of examples $S_n = \mathrm{End}_C(X^{\otimes n})$

Other examples we know come from 2-representation theory and fusion categories



Example

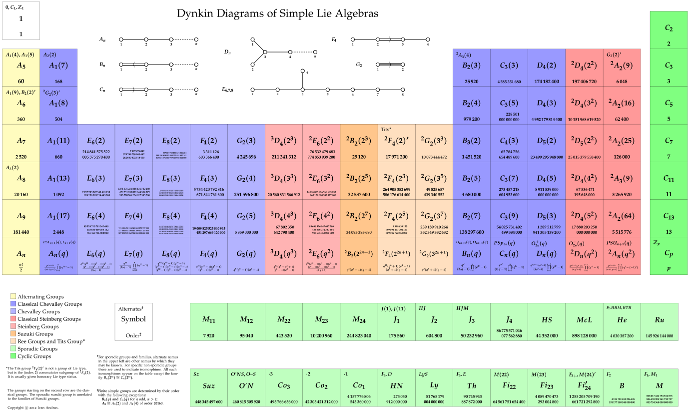
A measure of whether a monoid resists linear attacks is the representation gap:

The minimal m such that $M \ncong \mathbb{1}_{bt}^{\oplus k}$ with $\dim M = m$ exists

Up to extensions, the gap is $\min\{\dim L | L \text{ simple, non-trivial}\}$

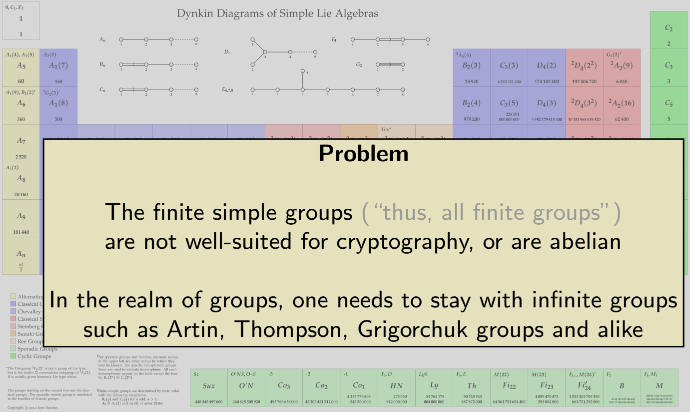
- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^x$

Examples and non-examples



- **Classical examples** Cyclic groups have only big representations over $\mathbb{F}_p$
- **Non-examples** Groups of Lie type have all very small representations
- **Non-examples** Sporadic groups are too small to be useful

Examples and non-examples



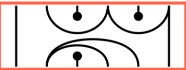
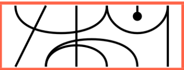
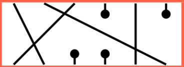
Problem

The finite simple groups (“thus, all finite groups”)
are not well-suited for cryptography, or are abelian

In the realm of groups, one needs to stay with infinite groups
such as Artin, Thompson, Grigorchuk groups and alike

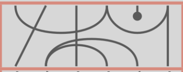
- Classical examples Cyclic groups have only big representations over $\mathbb{F}_p$
- Non-examples Groups of Lie type have all very small representations
- Non-examples Sporadic groups are too small to be useful

Examples and non-examples

Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
pPa_n		YES*	Pa_n		YES*
Mo_n		YES	$RoBr_n$		YES*
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

- **New examples** Finite monoids coming from quantum topology
- **More specific** Submonoids of the partition monoid above
- **Completely open** I claim your favorite example from quantum topology will also work

Examples and non-examples

Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
pPa_n		YES*	Pa_n		YES*
Mo_n		YES	$RoBr_n$		YES*
T					
pl					
p					

Task

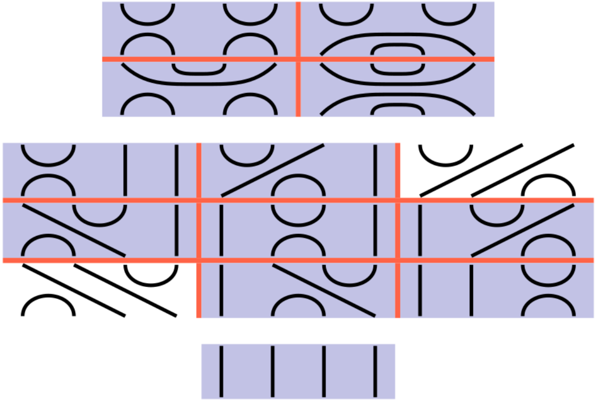
Find good lower bounds and growth rates for the representation gap

Observation

This is completely open, even for groups:
in representation theory researchers prefer(?) precise numbers
and bounds are not very common

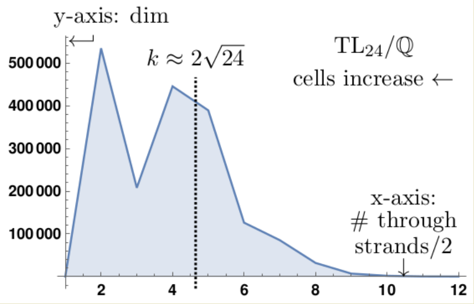
- New examples Finite monoids coming from quantum topology
- More specific Submonoids of the partition monoid above
- Completely open I claim your favorite example from quantum topology will also work

Temperley–Lieb works!



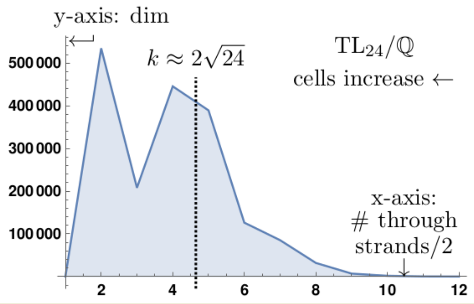
- Monoidal category example The Temperley–Lieb monoid TL_n (circle=1)
- TL_n has one simple L_k per cell $k =$ through strands
- Extensions $\mathbb{1}_{bt} \to M \to \mathbb{1}_{bt}$ are all trivial

Dimensions of simple TL_{24}-representations



- Monoidal category example The Temperley–Lieb monoid TL_n (circle=1)
- TL_n has one simple L_k per cell k = through strands
- Extensions $\mathbb{1}_{bt} \to M \to \mathbb{1}_{bt}$ are all trivial

Dimensions of simple TL_{24}-representations

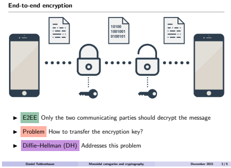


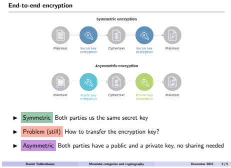
Example (following Spencer ∼2021)

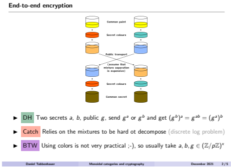
After appropriate truncation
the representation gap of TL_n is bounded from below by

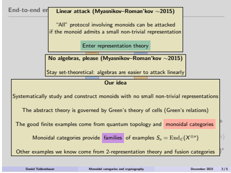
$$\frac{4}{(n+\lfloor 2\sqrt{n}\rfloor+2)(n+\lfloor 2\sqrt{n}\rfloor+4)}\binom{n}{(n+\lfloor 2\sqrt{n}\rfloor)/2}$$

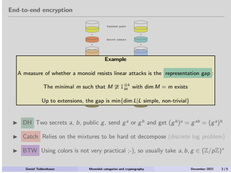
- Monoida … (circle=1)
- TL_n has …
- Extensions $\mathbb{1}_{bt} \to M \to \mathbb{1}_{bt}$ are all trivial

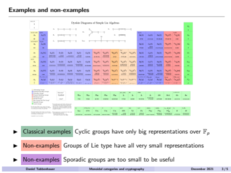


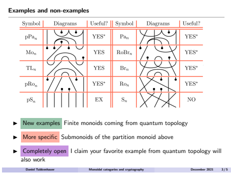


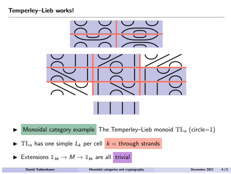


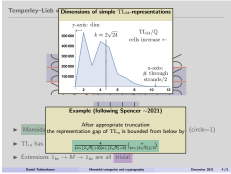




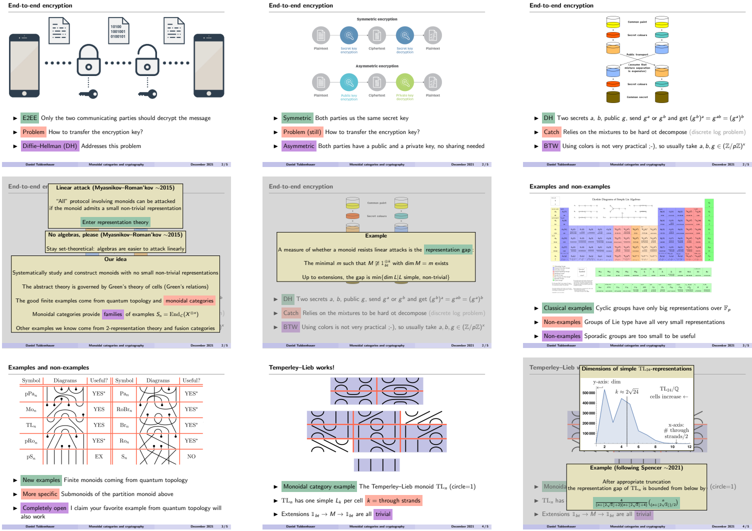








There is still much to do...



Thanks for your attention!