

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 encryption

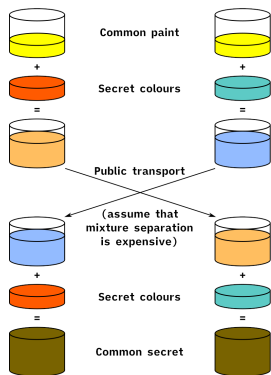


Asymmetric encryption



- ▶ **Symmetric** Both parties use 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



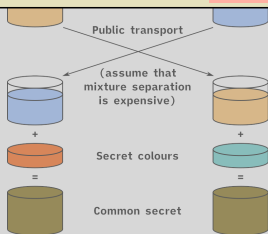
- ▶ **DH** Two secrets a, b , public g , send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- ▶ **Catch** Relies on the mixtures to be hard to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

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 to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

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

Public transport

(assume that)

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

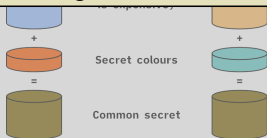
Linear attack (Myasnikov–Roman'kov ~2015)

“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 to 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

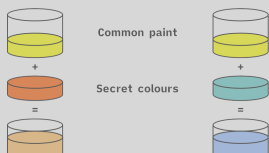
The abstract theory is governed by Green's theory of cells (Green's relations)

The good finite examples come from quantum topology and **monoidal categories**

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

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

End-to-end encryption



Example

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

The minimal m such that $M \not\cong \mathbb{1}_{bt}^{\oplus k}$ with $\dim M = m$ exists

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

- ▶ **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 to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical ;-), so usually take $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

Examples and non-examples

| \mathfrak{g}, C_2, Z_2 | Dynkin Diagrams of Simple Lie Algebras | | | | | | | | | | | | | | | C_2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|--|-------|--|-------|--|-------|--|-------|--|-------|--|-------|--|-------|--|-------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|--|-----------|
| A_1 | | A_2 | | A_3 | | A_4 | | A_5 | | A_6 | | A_7 | | A_8 | | A_9 | | A_{10} | | A_{11} | | A_{12} | | A_{13} | | A_{14} | | A_{15} | | A_{16} | | A_{17} | | A_{18} | | A_{19} | | A_{20} | | A_{21} | | A_{22} | | A_{23} | | A_{24} | | A_{25} | | A_{26} | | A_{27} | | A_{28} | | A_{29} | | A_{30} | | A_{31} | | A_{32} | | A_{33} | | A_{34} | | A_{35} | | A_{36} | | A_{37} | | A_{38} | | A_{39} | | A_{40} | | A_{41} | | A_{42} | | A_{43} | | A_{44} | | A_{45} | | A_{46} | | A_{47} | | A_{48} | | A_{49} | | A_{50} | | A_{51} | | A_{52} | | A_{53} | | A_{54} | | A_{55} | | A_{56} | | A_{57} | | A_{58} | | A_{59} | | A_{60} | | A_{61} | | A_{62} | | A_{63} | | A_{64} | | A_{65} | | A_{66} | | A_{67} | | A_{68} | | A_{69} | | A_{70} | | A_{71} | | A_{72} | | A_{73} | | A_{74} | | A_{75} | | A_{76} | | A_{77} | | A_{78} | | A_{79} | | A_{80} | | A_{81} | | A_{82} | | A_{83} | | A_{84} | | A_{85} | | A_{86} | | A_{87} | | A_{88} | | A_{89} | | A_{90} | | A_{91} | | A_{92} | | A_{93} | | A_{94} | | A_{95} | | A_{96} | | A_{97} | | A_{98} | | A_{99} | | A_{100} | | A_{101} | | A_{102} | | A_{103} | | A_{104} | | A_{105} | | A_{106} | | A_{107} | | A_{108} | | A_{109} | | A_{110} | | A_{111} | | A_{112} | | A_{113} | | A_{114} | | A_{115} | | A_{116} | | A_{117} | | A_{118} | | A_{119} | | A_{120} | | A_{121} | | A_{122} | | A_{123} | | A_{124} | | A_{125} | | A_{126} | | A_{127} | | A_{128} | | A_{129} | | A_{130} | | A_{131} | | A_{132} | | A_{133} | | A_{134} | | A_{135} | | A_{136} | | A_{137} | | A_{138} | | A_{139} | | A_{140} | | A_{141} | | A_{142} | | A_{143} | | A_{144} | | A_{145} | | A_{146} | | A_{147} | | A_{148} | | A_{149} | | A_{150} | | A_{151} | | A_{152} | | A_{153} | | A_{154} | | A_{155} | | A_{156} | | A_{157} | | A_{158} | | A_{159} | | A_{160} | | A_{161} | | A_{162} | | A_{163} | | A_{164} | | A_{165} | | A_{166} | | A_{167} | | A_{168} | | A_{169} | | A_{170} | | A_{171} | | A_{172} | | A_{173} | | A_{174} | | A_{175} | | A_{176} | | A_{177} | | A_{178} | | A_{179} | | A_{180} | | A_{181} | | A_{182} | | A_{183} | | A_{184} | | A_{185} | | A_{186} | | A_{187} | | A_{188} | | A_{189} | | A_{190} | | A_{191} | | A_{192} | | A_{193} | | A_{194} | | A_{195} | | A_{196} | | A_{197} | | A_{198} | | A_{199} | | A_{200} | | A_{201} | | A_{202} | | A_{203} | | A_{204} | | A_{205} | | A_{206} | | A_{207} | | A_{208} | | A_{209} | | A_{210} | | A_{211} | | A_{212} | | A_{213} | | A_{214} | | A_{215} | | A_{216} | | A_{217} | | A_{218} | | A_{219} | | A_{220} | | A_{221} | | A_{222} | | A_{223} | | A_{224} | | A_{225} | | A_{226} | | A_{227} | | A_{228} | | A_{229} | | A_{230} | | A_{231} | | A_{232} | | A_{233} | | A_{234} | | A_{235} | | A_{236} | | A_{237} | | A_{238} | | A_{239} | | A_{240} | | A_{241} | | A_{242} | | A_{243} | | A_{244} | | A_{245} | | A_{246} | | A_{247} | | A_{248} | | A_{249} | | A_{250} | | A_{251} | | A_{252} | | A_{253} | | A_{254} | | A_{255} | | A_{256} | | A_{257} | | A_{258} | | A_{259} | | A_{260} | | A_{261} | | A_{262} | | A_{263} | | A_{264} | | A_{265} | | A_{266} | | A_{267} | | A_{268} | | A_{269} | | A_{270} | | A_{271} | | A_{272} | | A_{273} | | A_{274} | | A_{275} | | A_{276} | | A_{277} | | A_{278} | | A_{279} | | A_{280} | | A_{281} | | A_{282} | | A_{283} | | A_{284} | | A_{285} | | A_{286} | | A_{287} | | A_{288} | | A_{289} | | A_{290} | | A_{291} | | A_{292} | | A_{293} | | A_{294} | | A_{295} | | A_{296} | | A_{297} | | A_{298} | | A_{299} | | A_{300} | | A_{301} | | A_{302} | | A_{303} | | A_{304} | | A_{305} | | A_{306} | | A_{307} | | A_{308} | | A_{309} | | A_{310} | | A_{311} | | A_{312} | | A_{313} | | A_{314} | | A_{315} | | A_{316} | | A_{317} | | A_{318} | | A_{319} | | A_{320} | | A_{321} | | A_{322} | | A_{323} | | A_{324} | | A_{325} | | A_{326} | | A_{327} | | A_{328} | | A_{329} | | A_{330} | | A_{331} | | A_{332} | | A_{333} | | A_{334} | | A_{335} | | A_{336} | | A_{337} | | A_{338} | | A_{339} | | A_{340} | | A_{341} | | A_{342} | | A_{343} | | A_{344} | | A_{345} | | A_{346} | | A_{347} | | A_{348} | | A_{349} | | A_{350} | | A_{351} | | A_{352} | | A_{353} | | A_{354} | | A_{355} | | A_{356} | | A_{357} | | A_{358} | | A_{359} | | A_{360} | | A_{361} | | A_{362} | | A_{363} | | A_{364} | | A_{365} | | A_{366} | | A_{367} | | A_{368} | | A_{369} | | A_{370} | | A_{371} | | A_{372} | | A_{373} | | A_{374} | | A_{375} | | A_{376} | | A_{377} | | A_{378} | | A_{379} | | A_{380} | | A_{381} | | A_{382} | | A_{383} | | A_{384} | | A_{385} | | A_{386} | | A_{387} | | A_{388} | | A_{389} | | A_{390} | | A_{391} | | A_{392} | | A_{393} | | A_{394} | | A_{395} | | A_{396} | | A_{397} | | A_{398} | | A_{399} | | A_{400} | | A_{401} | | A_{402} | | A_{403} | | A_{404} | | A_{405} | | A_{406} | | A_{407} | | A_{408} | | A_{409} | | A_{410} | | A_{411} | | A_{412} | | A_{413} | | A_{414} | | A_{415} | | A_{416} | | A_{417} | | A_{418} | | A_{419} | | A_{420} | | A_{421} | | A_{422} | | A_{423} | | A_{424} | | A_{425} | | A_{426} | | A_{427} | | A_{428} | | A_{429} | | A_{430} | | A_{431} | | A_{432} | | A_{433} | | A_{434} | | A_{435} | | A_{436} | | A_{437} | | A_{438} | | A_{439} | | A_{440} | | A_{441} | | A_{442} | | A_{443} | | A_{444} | | A_{445} |

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* |

Task

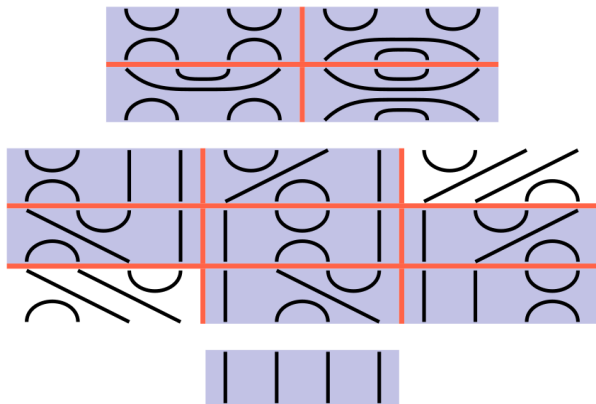
Find good lower bounds and growth rates for the representation gap

Observation

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

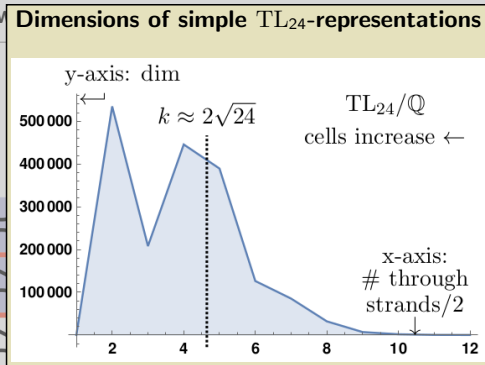
- ▶ New examples: finite monoids coming from quantum topology
- ▶ More specific: Submonoids of the partition monoid above
- ▶ Completely open: I claim your favorite example from quantum topology will also work

Temperley–Lieb works!



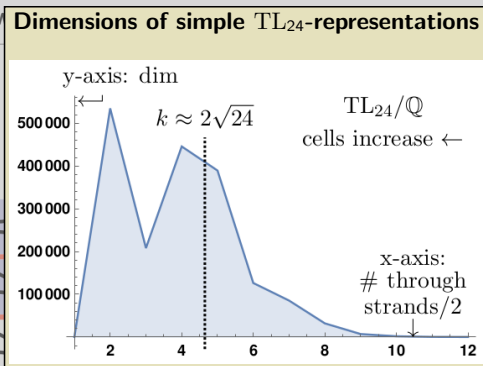
- ▶ Monoidal category example The Temperley–Lieb monoid TL_n (circle=1)
- ▶ TL_n has one simple L_k per cell $k = \text{through strands}$
- ▶ Extensions $\mathbb{1}_{bt} \rightarrow M \rightarrow \mathbb{1}_{bt}$ are all trivial

Temperley–Lieb v 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 $k = \text{through strands}$
- ▶ Extensions $\mathbb{1}_{bt} \rightarrow M \rightarrow \mathbb{1}_{bt}$ are all trivial

Temperley–Lieb v Dimensions of simple TL_{24} -representations



Example (following Spencer ~2021)

After appropriate truncation the representation gap of TL_n is bounded from below by (circle=1)

▶ Monoidal

▶ TL_n has

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

▶ Extensions $\mathbb{1}_{bt} \rightarrow M \rightarrow \mathbb{1}_{bt}$ are all trivial

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end

Linear attack (Miyake-Ruan'2015)

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

Enter representation theory

No algebras, please (Miyake-Ruan'2015)

Stay not-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 $S = \text{End}(X^{\otimes n})$

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Examples and non-examples

| Symbol | Diagram | Useful? | Synthesized | Diagram | Useful? |
|-----------------|---------|---------|-----------------|---------|---------|
| $\mathbb{P}N_n$ | | YES* | $\mathbb{P}n$ | | YES* |
| M_n | | YES | $\text{Rfd}n_1$ | | YES* |
| TL_n | | YES | B_n | | YES* |
| $\mathbb{P}B_n$ | | YES* | B_n | | YES* |
| $\mathbb{P}S_n$ | | EX | S_n | | NO |

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption

Example

A measure of whether a monoid admits linear attacks is the **representation gap**.

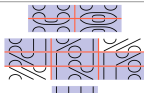
The minimal n such that $M \cong \mathbb{Z}^n$ with $\dim M = n$ exists

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

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Temperley-Lieb works!



- **Monoidal category example** The Temperley-Lieb monoid TL_n (circle=1)
- TL_n has one simple $\mathbb{1}_k$ per cell $k = \text{through strands}$
- Extensions $1_{\mu} \rightarrow M \rightarrow 1_{\mu}$ are all **trivial**

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Temperley-Lieb **Dimension of simple TL_n -representations**

n -axis: \dim

$\theta = 2\sqrt{3}$

TL_n/Q cells increase \leftarrow

n -axis: $\#$ strands $\text{strands}/2$

Example (following Spencer – 2021)

After appropriate truncation the representation gap of TL_n is bounded from below by $\left(\frac{n-1}{2}\right)_{\theta}$ (circle=1)

- **BTW** TL_n has $\dim \mathbb{1}_k = \binom{n-1}{k}_{\theta}$
- Extensions $1_{\mu} \rightarrow M \rightarrow 1_{\mu}$ are all **trivial**

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

There is still much to do...

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end

Linear attack (Miyake-Ruan-kaw -2015)

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

Enter representation theory

No algebras, please (Miyake-Ruan-kaw -2015)

Stay not-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 $S = \text{End}(X^{\otimes n})$

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Examples and non-examples

| Symbol | Diagram | Useful? | Synthesized | Diagram | Useful? |
|-----------|---------|---------|----------------|---------|---------|
| μP_n | | YES* | P_n | | YES* |
| M_n | | YES | $\text{Rd}P_n$ | | YES* |
| TL_n | | YES | B_n | | YES* |
| μB_n | | YES* | B_n | | YES* |
| μS_n | | EX | S_n | | NO |

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption



Example

A measure of whether a monoid admits linear attacks is the **representation gap**.

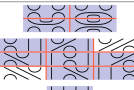
The minimal n such that $M \cong \mathbb{Z}^n$ with $\dim M = n$ exists

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

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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Temperley-Lieb works!



- **Monoidal category example** The Temperley-Lieb monoid TL_n (circle=1)
- TL_n has one simple $\mathbb{1}_k$ per cell $k = \text{through strands}$
- Extensions $1_\mu \rightarrow M \rightarrow 1_\mu$ are all **trivial**

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

End-to-end encryption



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

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Examples and non-examples

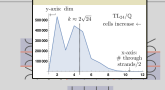


- **Classical examples** Cyclic groups have only big representations over \mathbb{F}_p
- **Non-examples** Groups of Lie type have all very small representations
- **Non-examples** Sporadic groups are too small to be useful

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Temperley-Lieb

Dimension of simple TL_n -representations



Example (following Spencer -2021)

- **Illustration** After appropriate truncation the representation gap of TL_n is bounded from below by $\frac{n-1}{2}$ (circle=1)
- TL_n has $\frac{n-1}{2}$ simple $\mathbb{1}_k$ per cell $k = \text{through strands}$
- Extensions $1_\mu \rightarrow M \rightarrow 1_\mu$ are all **trivial**

David Tubbenhauer Monoidal categories and cryptography December 2021 5/15

Thanks for your attention!