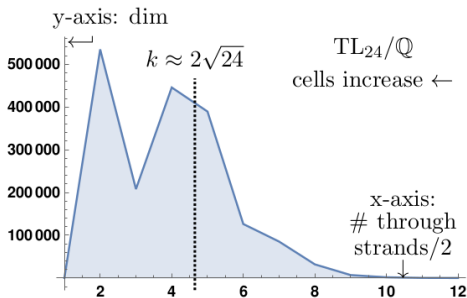


# Monoidal categories, representation gap and cryptography

Or: Why I like dimensions

Daniel Tubbenhauer



Joint with Mikhail Khovanov and Maithreya Sitaraman

March 2022

# 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

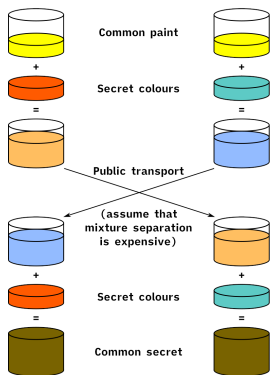


## Asymmetric encryption



- ▶ **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



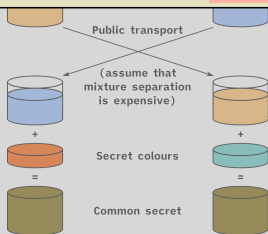
- ▶ **DH** Two secrets  $a, b$ , public  $g$ , send  $g^a$  or  $g^b$  and get  $(g^b)^a = g^{ab} = (g^a)^b$
- ▶ **Catch** Relies on the mixtures to be hard to decompose (discrete log problem)
- ▶ **BTW** Using colors is not practical ;-), so usually take  $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

## 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 practical ;-), so usually take  $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

## 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

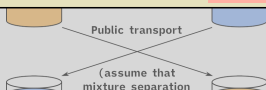
The complexity of  $S$  determines how difficult it is to find the common secret from the public data

## 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 (Stickel's (St) key exchange protocol)

The public data is a monoid  $S$ , and two noncommuting elements  $g, h \in S$ ,  $gh \neq hg$

Party A chooses privately  $a, a' \in \mathbb{N}$  and party B chooses privately  $b, b' \in \mathbb{N}$

Party A communicates  $g^a h^{a'}$ , B sends  $g^b h^{b'}$  and the common secret is  $g^a g^b h^{b'} h^{a'} = g^b g^a h^{a'} h^{b'}$

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

## End-to-end encryption

### 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

### Computers and fields

The important ground fields in this business are  $\mathbb{Q}$  or  $\mathbb{F}_q$   
(A computer doesn't know what  $\mathbb{R}$  or  $\mathbb{C}$  are)

- ▶ **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 practical ;-), so usually take  $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^\times$



### 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  $S_n = \text{End}_C(X^{\otimes n})$

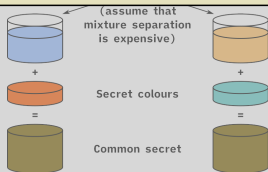
Other examples we know come from 2-representation theory and fusion categories

## A measure

A measure of whether a monoid resists linear attacks is the **representation gap**  $\text{gap}_{\mathbb{K}}(S)$ :

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 practical ;-), so usually take  $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

# End-to-end encryption

## A measure

A measure of whether a monoid resists linear attacks is the **representation gap**  $\text{gap}_{\mathbb{K}}(S)$ :

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

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



## The point

Make a list of families of monoids  $S_n$  with large  $\text{gap}_{\mathbb{K}}(S_n)$  compared to  $|S_n|$

▶ **DH** Two secret

▶ **Catch** Relies

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

Whether these are really useful for cryptography is a question for later ;-)

$$b)^a = g^{ab} = (g^a)^b$$

crete log problem)

# Examples and non-examples

$\mathfrak{sl}_2(\mathbb{C})$   
 $\mathfrak{sl}_2$   
 $\mathfrak{sl}_2$

### Dynkin Diagrams of Simple Lie Algebras

$C_2$   
 $C_2$   
 $C_2$

$A_0(\mathfrak{sl}_1), A_1(\mathfrak{sl}_2)$	$A_2(\mathfrak{sl}_3)$	$A_3(\mathfrak{sl}_4)$	$A_4(\mathfrak{sl}_5)$	$A_5(\mathfrak{sl}_6)$	$A_6(\mathfrak{sl}_7)$	$A_7(\mathfrak{sl}_8)$	$A_8(\mathfrak{sl}_9)$	$A_9(\mathfrak{sl}_{10})$	$A_{10}(\mathfrak{sl}_{11})$	$A_{11}(\mathfrak{sl}_{12})$	$A_{12}(\mathfrak{sl}_{13})$	$A_{13}(\mathfrak{sl}_{14})$	$A_{14}(\mathfrak{sl}_{15})$	$A_{15}(\mathfrak{sl}_{16})$	$A_{16}(\mathfrak{sl}_{17})$	$A_{17}(\mathfrak{sl}_{18})$	$A_{18}(\mathfrak{sl}_{19})$	$A_{19}(\mathfrak{sl}_{20})$	$A_{20}(\mathfrak{sl}_{21})$	$A_{21}(\mathfrak{sl}_{22})$	$A_{22}(\mathfrak{sl}_{23})$	$A_{23}(\mathfrak{sl}_{24})$	$A_{24}(\mathfrak{sl}_{25})$	$A_{25}(\mathfrak{sl}_{26})$	$A_{26}(\mathfrak{sl}_{27})$	$A_{27}(\mathfrak{sl}_{28})$	$A_{28}(\mathfrak{sl}_{29})$	$A_{29}(\mathfrak{sl}_{30})$	$A_{30}(\mathfrak{sl}_{31})$	$A_{31}(\mathfrak{sl}_{32})$	$A_{32}(\mathfrak{sl}_{33})$	$A_{33}(\mathfrak{sl}_{34})$	$A_{34}(\mathfrak{sl}_{35})$	$A_{35}(\mathfrak{sl}_{36})$	$A_{36}(\mathfrak{sl}_{37})$	$A_{37}(\mathfrak{sl}_{38})$	$A_{38}(\mathfrak{sl}_{39})$	$A_{39}(\mathfrak{sl}_{40})$	$A_{40}(\mathfrak{sl}_{41})$	$A_{41}(\mathfrak{sl}_{42})$	$A_{42}(\mathfrak{sl}_{43})$	$A_{43}(\mathfrak{sl}_{44})$	$A_{44}(\mathfrak{sl}_{45})$	$A_{45}(\mathfrak{sl}_{46})$	$A_{46}(\mathfrak{sl}_{47})$	$A_{47}(\mathfrak{sl}_{48})$	$A_{48}(\mathfrak{sl}_{49})$	$A_{49}(\mathfrak{sl}_{50})$	$A_{50}(\mathfrak{sl}_{51})$	$A_{51}(\mathfrak{sl}_{52})$	$A_{52}(\mathfrak{sl}_{53})$	$A_{53}(\mathfrak{sl}_{54})$	$A_{54}(\mathfrak{sl}_{55})$	$A_{55}(\mathfrak{sl}_{56})$	$A_{56}(\mathfrak{sl}_{57})$	$A_{57}(\mathfrak{sl}_{58})$	$A_{58}(\mathfrak{sl}_{59})$	$A_{59}(\mathfrak{sl}_{60})$	$A_{60}(\mathfrak{sl}_{61})$	$A_{61}(\mathfrak{sl}_{62})$	$A_{62}(\mathfrak{sl}_{63})$	$A_{63}(\mathfrak{sl}_{64})$	$A_{64}(\mathfrak{sl}_{65})$	$A_{65}(\mathfrak{sl}_{66})$	$A_{66}(\mathfrak{sl}_{67})$	$A_{67}(\mathfrak{sl}_{68})$	$A_{68}(\mathfrak{sl}_{69})$	$A_{69}(\mathfrak{sl}_{70})$	$A_{70}(\mathfrak{sl}_{71})$	$A_{71}(\mathfrak{sl}_{72})$	$A_{72}(\mathfrak{sl}_{73})$	$A_{73}(\mathfrak{sl}_{74})$	$A_{74}(\mathfrak{sl}_{75})$	$A_{75}(\mathfrak{sl}_{76})$	$A_{76}(\mathfrak{sl}_{77})$	$A_{77}(\mathfrak{sl}_{78})$	$A_{78}(\mathfrak{sl}_{79})$	$A_{79}(\mathfrak{sl}_{80})$	$A_{80}(\mathfrak{sl}_{81})$	$A_{81}(\mathfrak{sl}_{82})$	$A_{82}(\mathfrak{sl}_{83})$	$A_{83}(\mathfrak{sl}_{84})$	$A_{84}(\mathfrak{sl}_{85})$	$A_{85}(\mathfrak{sl}_{86})$	$A_{86}(\mathfrak{sl}_{87})$	$A_{87}(\mathfrak{sl}_{88})$	$A_{88}(\mathfrak{sl}_{89})$	$A_{89}(\mathfrak{sl}_{90})$	$A_{90}(\mathfrak{sl}_{91})$	$A_{91}(\mathfrak{sl}_{92})$	$A_{92}(\mathfrak{sl}_{93})$	$A_{93}(\mathfrak{sl}_{94})$	$A_{94}(\mathfrak{sl}_{95})$	$A_{95}(\mathfrak{sl}_{96})$	$A_{96}(\mathfrak{sl}_{97})$	$A_{97}(\mathfrak{sl}_{98})$	$A_{98}(\mathfrak{sl}_{99})$	$A_{99}(\mathfrak{sl}_{100})$																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					
1	6	20	42	70	105	153	216	297	399	528	688	882	1125	1430	1800	2250	2805	3480	4290	5250	6384	7700	9216	10950	12930	15180	17730	20610	23850	27480	31530	36135	41340	47205	53790	61165	69390	78540	88695	99930	112350	126045	141000	157305	174960	194005	214470	236385	259780	284695	311160	339215	368910	399285	430380	462135	494600	527825	561860	596655	632160	668325	705110	742575	780680	819385	858650	898435	938710	979445	1020600	1062135	1104010	1146285	1188920	1231875	1275110	1318585	1362270	1406125	1450120	1494225	1538410	1582645	1626990	1671415	1715890	1760475	1805140	1849845	1894560	1939265	1983930	2028525	2073030	2117515	2161960	2206335	2250610	2294765	2338770	2382685	2426490	2470155	2513650	2556945	2599990	2642765	2685140	2727085	2768570	2809565	2849940	2889665	2928710	2967045	3004640	3041365	3077190	3112085	3145920	3178665	3210290	3240765	3270060	3298145	3324990	3350575	3374870	3397845	3419470	3439715	3458560	3475975	3491930	3506405	3519370	3530805	3540690	3549005	3555730	3560845	3565330	3569165	3572330	3574805	3576570	3577605	3577900	3577445	3576230	3574235	3571450	3567855	3563440	3558185	3552070	3545075	3537190	3528405	3518710	3508105	3496570	3484085	3470640	3456225	3440830	3424445	3407060	3388665	3369250	3348805	3327320	3304785	3281190	3256525	3230780	3203945	3176010	3146965	3116800	3085505	3053070	3019485	2984740	2948825	2911740	2873475	2833930	2793095	2750960	2707515	2662760	2616695	2569320	2520635	2470640	2419335	2366710	2312765	2257490	2200885	2142950	2083675	2023060	1960105	1895810	1830175	1763200	1694885	1625230	1554235	1481900	1408225	1333210	1256855	1179160	1099125	1016750	933035	847980	761585	673850	584775	494360	402605	310510	219075	128300	38145	-51710	-151715	-251770	-351225	-449080	-545335	-638990	-729045	-815500	-897355	-974610	-1047265	-1115320	-1177775	-1234630	-1285885	-1331540	-1371695	-1406350	-1435505	-1459160	-1477315	-1490870	-1499825	-1504180	-1503935	-1499190	-1489945	-1476200	-1447955	-1405210	-1348965	-1280220	-1198975	-1106230	-1002985	-889240	-765195	-631750	-488905	-336660	-175015	-10000	100000	300000	500000	700000	900000	1100000	1300000	1500000	1700000	1900000	2100000	2300000	2500000	2700000	2900000	3100000	3300000	3500000	3700000	3900000	4100000	4300000	4500000	4700000	4900000	5100000	5300000	5500000	5700000	5900000	6100000	6300000	6500000	6700000	6900000	7100000	7300000	7500000	7700000	7900000	8100000	8300000	8500000	8700000	8900000	9100000	9300000	9500000	9700000	9900000	10100000	10300000	10500000	10700000	10900000	11100000	11300000	11500000	11700000	11900000	12100000	12300000	12500000	12700000	12900000	13100000	13300000	13500000	13700000	13900000	14100000	14300000	14500000	14700000	14900000	15100000	15300000	15500000	15700000	15900000	16100000	16300000	16500000	16700000	16900000	17100000	17300000	17500000	17700000	17900000	18100000	18300000	18500000	18700000	18900000	19100000	19300000	19500000	19700000	19900000	20100000	20300000	20500000	20700000	20900000	21100000	21300000	21500000	21700000	21900000	22100000	22300000	22500000	22700000	22900000	23100000	23300000	23500000	23700000	23900000	24100000	24300000	24500000	24700000	24900000	25100000	25300000	25500000	25700000	25900000	26100000	26300000	26500000	26700000	26900000	27100000	27300000	27500000	27700000	27900000	28100000	28300000	28500000	28700000	28900000	29100000	29300000	29500000	29700000	29900000	30100000	30300000	30500000	30700000	30900000	31100000	31300000	31500000	31700000	31900000	32100000	32300000	32500000	32700000	32900000	33100000	33300000	33500000	33700000	33900000	34100000	34300000	34500000	34700000	34900000	35100000	35300000	35500000	35700000	35900000	36100000	36300000	36500000	36700000	36900000	37100000	37300000	37500000	37700000	37900000	38100000	38300000	38500000	38700000	38900000	39100000	39300000	39500000	39700000	39900000	40100000	40300000	40500000	40700000	40900000	41100000	41300000	41500000	41700000	41900000	42100000	42300000	42500000	42700000	42900000	43100000	43300000	43500000	43700000	43900000	44100000	44300000	44500000	44700000	44900000	45100000	45300000	45500000	45700000	45900000	46100000	46300000	46500000	46700000	46900000	47100000	47300000	47500000	47700000	47900000	48100000	48300000	48500000	48700000	48900000	49100000	49300000	49500000	49700000	49900000	50100000	50300000	50500000	50700000	50900000	51100000	51300000	51500000	51700000	51900000	52100000	52300000	52500000	52700000	52900000	53100000	53300000	53500000	53700000	53900000	54100000	54300000	54500000	54700000	54900000	55100000	55300000	55500000	55700000	55900000	56100000	56300000	56500000	56700000	56900000	57100000	57300000	57500000	57700000	57900000	58100000	58300000	58500000	58700000	58900000	59100000	59300000	59500000	59700000	59900000	60100000	60300000	60500000	60700000	60900000	61100000	61300000	61500000	61700000	61900000	62100000	62300000	62500000	62700000	62900000	63100000	63300000	63500000	63700000	63900000	64100000	64300000	64500000	64700000	64900000	65100000	65300000	65500000	65700000	65900000	66100000	66300000	66500000	66700000	66900000	67100000	67300000	67500000	67700000	67900000	68100000	68300000	68500000	68700000	68900000	69100000	69300000	69500000	69700000	69900000	70100000	70300000	70500000	70700000	70900000	71100000	71300000	71500000	71700000	71900000	72100000	72300000	72500000	72700000	72900000	73100000	73300000	73500000	73700000	73900000	74100000	74300000	74500000	74700000	74900000	75100000	75300000	75500000	75700000	75900000	76100000	76300000	76500000	76700000	76900000	77100000	77300000	77500000	77700000	77900000	78100000	78300000	78500000	78700000	78900000	79100000	79300000	79500000	79700000	79900000	80100000	80300000	80500000	80700000	80900000	81100000	81300000	81500000	81700000	81900000	82100000	82300000	82500000	82700000	82900000	83100000	83300000	83500000	83700000	83900000	84100000	84300000	84500000	84700000	84900000	85100000	85300000	85500000	85700000	85900000	86100000	86300000	86500000	86700000	86900000	87100000	87300000	87500000	87700000	87900000	88100000	88300000	88500000	88700000	88900000	89100000	89300000	89500000	89700000	89900000	90100000	90300000	90500000	90



# Examples and non-examples

Dynkin Diagrams of Simple Lie Algebras

$A_n$	$B_n$	$C_n$	$D_n$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$	$H_3$
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10

$A_n$	$B_n$	$C_n$	$D_n$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$	$H_3$
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10

Example ( $S_n =$  symmetric or alternating groups)

$\text{gap}_{\mathbb{K}}(S_n) \leq n$

since the permutation representation is  $n$ -dimensional

$n$  is very small compared to  $|S_n|$

\*The group  $S_n$  is a group of all permutations of  $n$  objects. It is a group of order  $n!$ . The group  $A_n$  is a group of all even permutations of  $n$  objects. It is a group of order  $n!/2$ .

The group  $S_n$  is a group of all permutations of  $n$  objects. It is a group of order  $n!$ . The group  $A_n$  is a group of all even permutations of  $n$  objects. It is a group of order  $n!/2$ .

The group  $S_n$  is a group of all permutations of  $n$  objects. It is a group of order  $n!$ . The group  $A_n$  is a group of all even permutations of  $n$  objects. It is a group of order  $n!/2$ .

- ▶ Classical examples Cyclic groups have a big representation gap over  $\mathbb{Q}$
- ▶ Non-examples Groups of Lie type have quite small representations
- ▶ Non-examples Sporadic groups are too sporadic to be useful

# Examples and non-examples

Dynkin Diagrams of Simple Lie Algebras

$A_n$	$B_n$	$C_n$	$D_n$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$	$H_4$
1	2	3	4	5	6	7	8	9	10

$A_n$	$B_n$	$C_n$	$D_n$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$	$H_4$
1	2	3	4	5	6	7	8	9	10

**Example ( $S_n, S_q = \text{SL}_n(\mathbb{F}_q)$  and  $\text{PSL}_n(\mathbb{F}_q)$ )**

$\text{gap}_{\mathbb{F}_q}(S_q) \leq n^2 - 1$   
 since they act on  $\mathbb{F}_q^n \otimes (\mathbb{F}_q^n)^* / \mathbb{F}_q$

$n^2 - 1$  is very small compared to  $|S_n|, |S_q|$

**Legend:**

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Special Groups
- Free Groups and Tits Groups
- Sporadic Groups
- Cyclic Groups

**Table of Simple Groups:**

$S_3$	$S_4$	$S_5$	$S_6$	$S_7$	$S_8$	$S_9$	$S_{10}$	$A_5$	$A_6$	$A_7$	$A_8$	$A_9$	$A_{10}$	$A_{11}$	$A_{12}$	$A_{13}$	$A_{14}$	$A_{15}$	$A_{16}$	$A_{17}$	$A_{18}$	$A_{19}$	$A_{20}$	$A_{21}$	$A_{22}$	$A_{23}$	$A_{24}$	$A_{25}$	$A_{26}$	$A_{27}$	$A_{28}$	$A_{29}$	$A_{30}$	$A_{31}$	$A_{32}$	$A_{33}$	$A_{34}$	$A_{35}$	$A_{36}$	$A_{37}$	$A_{38}$	$A_{39}$	$A_{40}$	$A_{41}$	$A_{42}$	$A_{43}$	$A_{44}$	$A_{45}$	$A_{46}$	$A_{47}$	$A_{48}$	$A_{49}$	$A_{50}$	$A_{51}$	$A_{52}$	$A_{53}$	$A_{54}$	$A_{55}$	$A_{56}$	$A_{57}$	$A_{58}$	$A_{59}$	$A_{60}$	$A_{61}$	$A_{62}$	$A_{63}$	$A_{64}$	$A_{65}$	$A_{66}$	$A_{67}$	$A_{68}$	$A_{69}$	$A_{70}$	$A_{71}$	$A_{72}$	$A_{73}$	$A_{74}$	$A_{75}$	$A_{76}$	$A_{77}$	$A_{78}$	$A_{79}$	$A_{80}$	$A_{81}$	$A_{82}$	$A_{83}$	$A_{84}$	$A_{85}$	$A_{86}$	$A_{87}$	$A_{88}$	$A_{89}$	$A_{90}$	$A_{91}$	$A_{92}$	$A_{93}$	$A_{94}$	$A_{95}$	$A_{96}$	$A_{97}$	$A_{98}$	$A_{99}$	$A_{100}$
-------	-------	-------	-------	-------	-------	-------	----------	-------	-------	-------	-------	-------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	-----------

- ▶ Classical examples Cyclic groups have a big representation gap over  $\mathbb{Q}$
- ▶ Non-examples Groups of Lie type have quite small representations
- ▶ Non-examples Sporadic groups are too sporadic to be useful







# Examples and non-examples

Dynkin Diagrams of Simple Lie Algebras

$A_n$	$B_n$	$C_n$	$D_n$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$	$H_4$	$C_2$
$A_1(3)$	$B_2(3)$	$C_3(3)$	$D_4(2)$	$G_2(3)$	$H_4(3)$	$G_2(3)$	$H_4(3)$	$H_4(3)$	$H_4(3)$	2
$A_2(6)$	$B_3(6)$	$C_4(4)$	$D_5(2)$	$G_2(4)$	$H_4(4)$	$G_2(4)$	$H_4(4)$	$H_4(4)$	$H_4(4)$	3
$A_3(10)$	$B_4(8)$	$C_5(5)$	$D_6(2)$	$G_2(5)$	$H_4(5)$	$G_2(5)$	$H_4(5)$	$H_4(5)$	$H_4(5)$	5
$A_4(15)$	$B_5(10)$	$C_6(6)$	$D_7(2)$	$G_2(6)$	$H_4(6)$	$G_2(6)$	$H_4(6)$	$H_4(6)$	$H_4(6)$	7
$A_5(21)$	$B_6(12)$	$C_7(7)$	$D_8(2)$	$G_2(7)$	$H_4(7)$	$G_2(7)$	$H_4(7)$	$H_4(7)$	$H_4(7)$	11
$A_6(28)$	$B_7(14)$	$C_8(8)$	$D_9(2)$	$G_2(8)$	$H_4(8)$	$G_2(8)$	$H_4(8)$	$H_4(8)$	$H_4(8)$	13
$A_7(36)$	$B_8(16)$	$C_9(9)$	$D_{10}(2)$	$G_2(9)$	$H_4(9)$	$G_2(9)$	$H_4(9)$	$H_4(9)$	$H_4(9)$	17
$A_8(45)$	$B_9(18)$	$C_{10}(10)$	$D_{11}(2)$	$G_2(10)$	$H_4(10)$	$G_2(10)$	$H_4(10)$	$H_4(10)$	$H_4(10)$	19
$A_9(55)$	$B_{10}(20)$	$C_{11}(11)$	$D_{12}(2)$	$G_2(11)$	$H_4(11)$	$G_2(11)$	$H_4(11)$	$H_4(11)$	$H_4(11)$	23
$A_{10}(66)$	$B_{11}(22)$	$C_{12}(12)$	$D_{13}(2)$	$G_2(12)$	$H_4(12)$	$G_2(12)$	$H_4(12)$	$H_4(12)$	$H_4(12)$	29

**Example ( $S_n =$  braid group in  $n$  strands)**

$\text{gap}_{\mathbb{K}}(S_n) \approx n$  or  $n(n-1)/2$

the dimensions of the Burau and the LKB representation

Too small

\*The "big gap" is not a gap in the usual sense, but it is a gap in the sense of the Burau and LKB representations.

- ▶ Classical examples Cyclic groups have a big representation gap over  $\mathbb{Q}$
- ▶ Non-examples Groups of Lie type have quite small representations
- ▶ Non-examples Sporadic groups are too sporadic 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
- ▶ **Widely 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

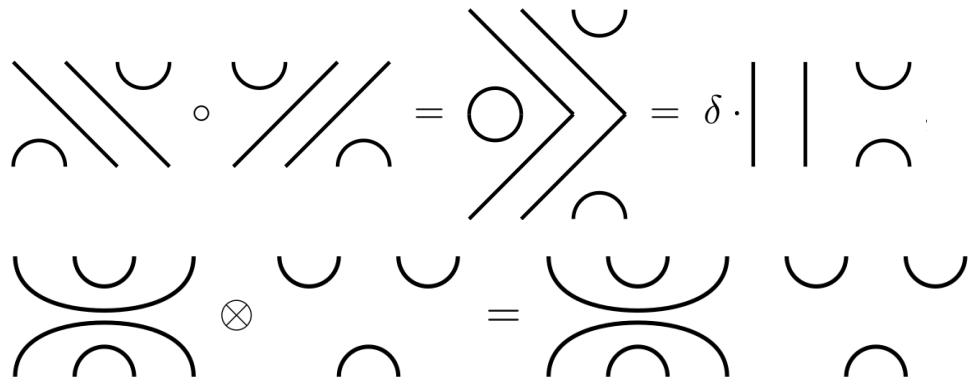
Find good lower bounds and growth rates for the representation gap

### Observation

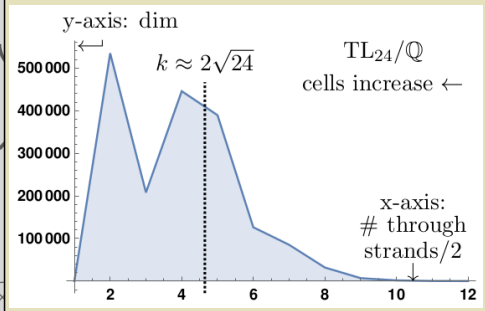
This is mostly open, even for groups:  
 in representation theory researchers prefer(?) precise numbers  
 and bounds are not very common

- ▶ New examples Finite monoids coming from quantum topology  
 I will zoom in on Temperley–Lieb now
- ▶ More specific Submonoids of the partition monoid above
- ▶ Widely open I claim your favorite example from quantum topology will also work

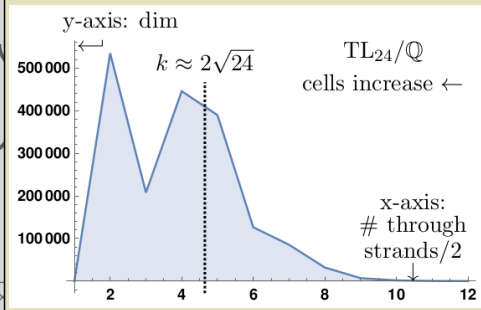
## Temperley–Lieb works!



- ▶ Monoidal category example The Temperley–Lieb monoid  $\mathrm{TL}_n$  (circle =  $\delta = 1$ )
- ▶  $\mathrm{TL}_n$  has one simple  $L_k$  per  $k \in \{n, n-2, \dots, 1 \text{ or } 0\}$  (through strands)
- ▶ Extensions  $\mathbb{1}_{bt} \rightarrow M \rightarrow \mathbb{1}_{bt}$  are all trivial

Dimensions of simple  $TL_{24}$ -representations

- ▶ Monoidal category example The Temperley–Lieb monoid  $TL_n$  (circle =  $\delta = 1$ )
- ▶  $TL_n$  has one simple  $L_k$  per  $k \in \{n, n-2, \dots, 1 \text{ or } 0\}$  (through strands)
- ▶ Extensions  $\mathbb{1}_{bt} \rightarrow M \rightarrow \mathbb{1}_{bt}$  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

$$\frac{4}{(n+\lfloor 2\sqrt{n} \rfloor + 2)(n+\lfloor 2\sqrt{n} \rfloor + 4)} \binom{n}{(n+\lfloor 2\sqrt{n} \rfloor)/2} \in \Theta(2^n n^{-5/2})$$

► Monoidal

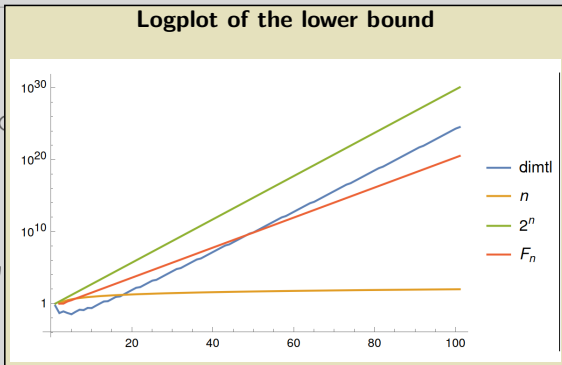
►  $TL_n$  has

► Extension

(circle =  $\delta = 1$ )

strands)

# Temperley–Lieb works!



## Example (following Spencer ~2021)

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

$$\frac{4}{(n + \lfloor 2\sqrt{n} \rfloor + 2)(n + \lfloor 2\sqrt{n} \rfloor + 4)} \binom{n}{(n + \lfloor 2\sqrt{n} \rfloor) / 2} \in \Theta(2^n n^{-5/2})$$

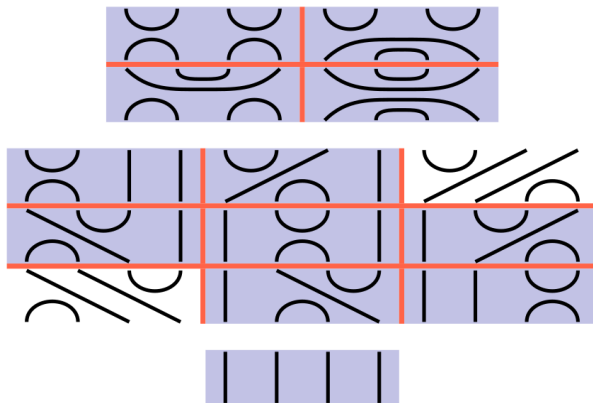
- ▶ Monoidal
- ▶  $TL_n$  has
- ▶ Extension

(circle =  $\delta = 1$ )  
strands



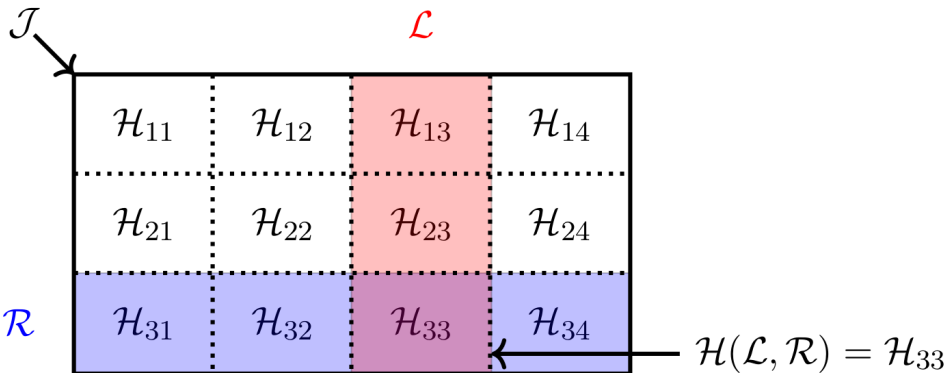
## The “How to” – some theory

---



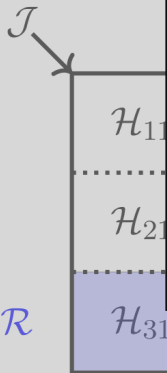
- ▶ Left order  $\leq_l$ :  $a \leq_l b \Leftrightarrow \exists c : b = ca$
- ▶ Left cells:  $(a \sim_l b) \Leftrightarrow (a \leq_l b \text{ and } b \leq_l a)$
- ▶ Right and two-sided are defined similar
- ▶ **Green cells** structure monoids

## The “How to” – some theory



- ▶ Left cells  $\mathcal{L}$
- ▶ Right cells  $\mathcal{R}$
- ▶ Two-sided cells  $\mathcal{J}$
- ▶ **H-cells** = intersection of a left and a right cell

The “How to” **Example (transformation monoid  $T_n = \text{End}(\{1, \dots, n\})$ )**



(111)
(222)
(333)
(122), (221)   (121), (212)   (221), (112)
(133), (331)   (313), (131)   (113), (311)
(233), (322)   (323), (232)   (223), (332)
(123), (213), (132)
(231), (312), (321)

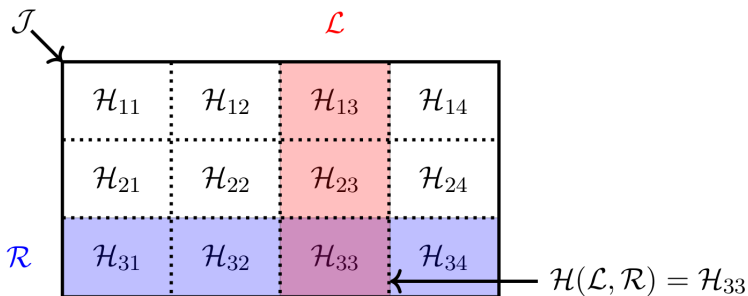
**Example ( $C_{3,2} = \langle a | a^{3+2} = a^3 \rangle$ )**

$a^3, a^4$
$a^2$
$a$
1

$\mathcal{H}(\mathcal{L}, \mathcal{R}) = \mathcal{H}_{33}$

- ▶ Left cells  $\mathcal{L}$
- ▶ Right cells  $\mathcal{R}$
- ▶ Two-sided cells  $\mathcal{J}$
- ▶  $H$ -cells = intersection

## The “How to” – some theory

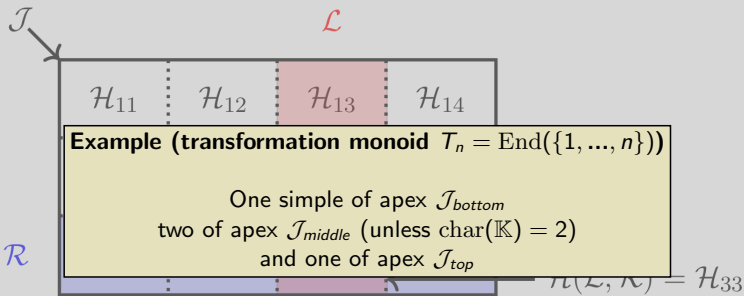


- ▶ If  $H$ -cells contain idempotents, then they are groups
- ▶ Each simple  $S$ -representation has an associated apex  $\mathcal{J}$
- ▶ Clifford–Munn–Ponizovskii theorem For a monoid  $S$ :

$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\} / \cong \xleftrightarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\} / \cong ,$$

where  $\mathcal{H}(e) \subset \mathcal{J}$  is any idempotent  $H$ -cell.

# The “How to” – some theory



- ▶ If  $H$ -cells contain idempotents, then they are groups
- ▶ Each simple  $S$ -rep
- ▶ Clifford–Munn–P

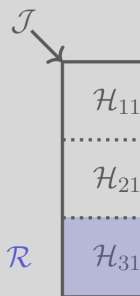
**Example ( $C_{3,2} = \langle a \mid a^{3+2} = a^3 \rangle$ )**

One simple of apex  $\mathcal{J}_{bottom}$   
 two of apex  $\mathcal{J}_{top}$  (unless  $\text{char}(\mathbb{K}) = 2$ )

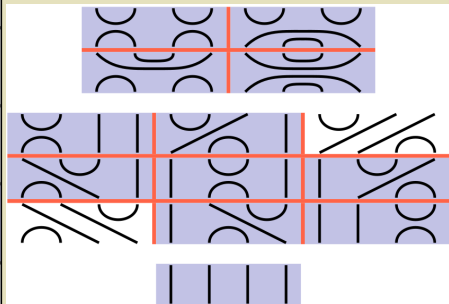
$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\} / \cong \xleftrightarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\} / \cong ,$$

where  $\mathcal{H}(e) \subset \mathcal{J}$  is any idempotent  $H$ -cell.

# The “How to” – some theory



## Example (back to Temperley–Lieb)



One simple of apex  $\mathcal{J}_k$   
 where  $k$  = number of through strands)

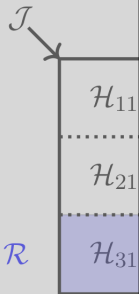
- ▶ If  $H$ -cells contain
- ▶ Each simple  $S$ -
- ▶ Clifford–Munn–Ponizovskiĭ theorem For a monoid  $S$ :

$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\} / \cong \xleftarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\} / \cong ,$$

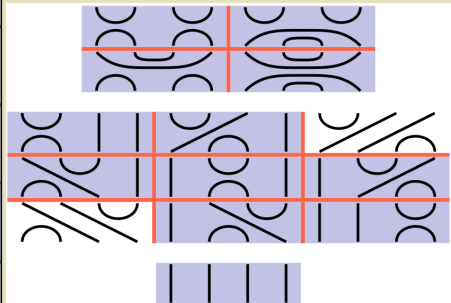
where  $\mathcal{H}(e) \subset \mathcal{J}$  is any idempotent  $H$ -cell.

$$\mathcal{C}, \mathcal{R}) = \mathcal{H}_{33}$$

# The “How to” – some theory



## Example (back to Temperley–Lieb)



One simple of apex  $\mathcal{J}_k$   
 where  $k$  = number of through strands)

- ▶ If  $H$ -cells contain
- ▶ Each simple  $S$ -
- ▶ Clifford–Mun

### Remark

Using Gram/pairing matrices (works in general)  
 one can compute the simple dimensions

$$\mathcal{C}, \mathcal{R}) = \mathcal{H}_{33}$$

{simple  $S$ -representations} /  $\cong$  ,

where  $\mathcal{H}(e) \subset \mathcal{J}$  is any idempotent  $H$ -cell.

### End-to-end encryption



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

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### End-to-end encryption



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

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### End-to-end encryption



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

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### End-to-end encryption

**Linear attack (Miyazaki-Rusakov – 2015)**  
 "All" protocol involving monoids can be attacked if the monoid admits a small non-trivial representation

Enter representation theory

No algebras, please (Miyazaki-Rusakov – 2015)  
 Stay on-theoretical: algebras are easier to attack linearly

**Our idea**  
 Systematically study and construct monoids with as small non-trivial representations

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

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

Monoidal categories provide **families** of examples  $S_n \subseteq \text{Equiv}(X^{[n]})$

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

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### Examples and non-examples



- **Classical examples** Cyclic groups have a big representation gap over  $\mathbb{Q}$
- **Non-examples** Groups of Lie type have quite small representations
- **Non-examples** Sporadic groups are too sporadic to be useful

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$p\mathbb{N}$		YES*	$\mathbb{P}^1$		YES*
$M_n$		YES	$Bd_n$		YES*
$TL_n$		YES	$B_n$		YES*
$p\mathbb{N}$		YES*	$B_n$		YES*
$p\mathbb{N}$		EX	$S_n$		NO

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

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### Temperley-Lieb

**Dimension of simple  $TL_n$ -representations**

$\lambda$ -axis: dim  
 $\delta \approx 2.52$   $TL_n/\mathbb{Q}$  rels increase  $\leftarrow$   
 $\mu$ -axis:  $\mu$  through strands  $\rightarrow$

**Example (following Speiser – 2021)**  
 After appropriate truncation the representation gap of  $TL_n$  is bounded from below by strands

(circle:  $\delta = 1$ )

►  $TL_n$  has  $\dim \text{Hom}(V_\lambda, V_\mu) \in \mathcal{O}(2^{\mu/\delta} \lambda^{\delta/\delta})$

► Extension  $\dim \text{Hom}(V_\lambda, V_\mu) \in \mathcal{O}(2^{\mu/\delta} \lambda^{\delta/\delta})$

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### Temperley-Lieb works!

**Logplot of the lower bound**

**Example (following Speiser – 2021)**  
 After appropriate truncation the representation gap of  $TL_n$  is bounded from below by strands

(circle:  $\delta = 1$ )

►  $TL_n$  has  $\dim \text{Hom}(V_\lambda, V_\mu) \in \mathcal{O}(2^{\mu/\delta} \lambda^{\delta/\delta})$

► Extension  $\dim \text{Hom}(V_\lambda, V_\mu) \in \mathcal{O}(2^{\mu/\delta} \lambda^{\delta/\delta})$

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

### The "How to" – some theory

- Left order  $S_2: a \circ S_1 \circ b \Leftrightarrow \mathbb{3}c: b = ca$
- Left call:  $(a \approx b) \Leftrightarrow (a \circ S_1) \circ b$  and  $b \circ S_1 \circ a$
- Right and two-sided an defined similar
- **Green cells** structure monoids

Basel University - Monoidal categories, representation gap and cryptography - March 2022 - 6/6

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)** Address this problem

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### End-to-end encryption



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

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### End-to-end encryption



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

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### End-to-end encryption

**Linear attack (Miyazaki-Rosen'kov – 2015)**

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

Enter representation theory

No algebras, please (Miyazaki-Rosen'kov – 2015)

Stay as theoretical as possible to attack linearly

**Our idea**

Systematically study and construct monoids with as small non-trivial representations

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

The good favorite examples come from quantum topology and monoidal categories

Monoidal categories provide families of examples  $S_n = \text{Eas}_n(X^{(n)})$

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

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### Examples and non-examples



- **Classical examples** Cyclic groups have a big representation gap over  $\mathbb{Q}$
- **Non-examples** Groups of Lie type have quite small representations
- **Non-examples** Sporadic groups are too sporadic to be useful

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$p\mathbb{Z}_n$		YES*	$\mathbb{P}^n$		YES*
$M_n$		YES	$\text{Rep}_n$		YES*
$TL_n$		YES	$B_n$		YES*
$pB_n$		YES*	$B_n^*$		YES*
$pS_n$		EX	$S_n$		NO

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

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### Temperley-Lieb

**Dimension of simple  $TL_n$ -representations**

$\lambda$ -axis: dim

$\delta \approx 2.471$   $TL_n/\mathbb{Q}$  rels increase  $\leftarrow$

$\lambda$ -axis:  $\beta$  through strands  $\rightarrow 2$

**Example (following Speiser – 2021)**

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

(circle:  $\delta = 1$ )

- $TL_n$  has
- Extensive

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### Temperley-Lieb works!

**Logplot of the lower bound**

**Example (following Speiser – 2021)**

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

(circle:  $\delta = 1$ )

- $TL_n$  has
- Extensive

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

### The "How to" – some theory

- Left order  $S_n: a \leq b \Leftrightarrow \exists c: b = ca$
- Left call:  $(a \sim b) \Leftrightarrow (a \leq b \text{ and } b \leq a)$
- Right and two-sided an defined similar
- **Green cells** structure monoids

Basel University, Max Planck Institute for Mathematics in the Sciences, March 2022, 6/18

Thanks for your attention!