

# Diagrammatics and cryptography

Or: Not too small, please!

Daniel Tubbenhauer

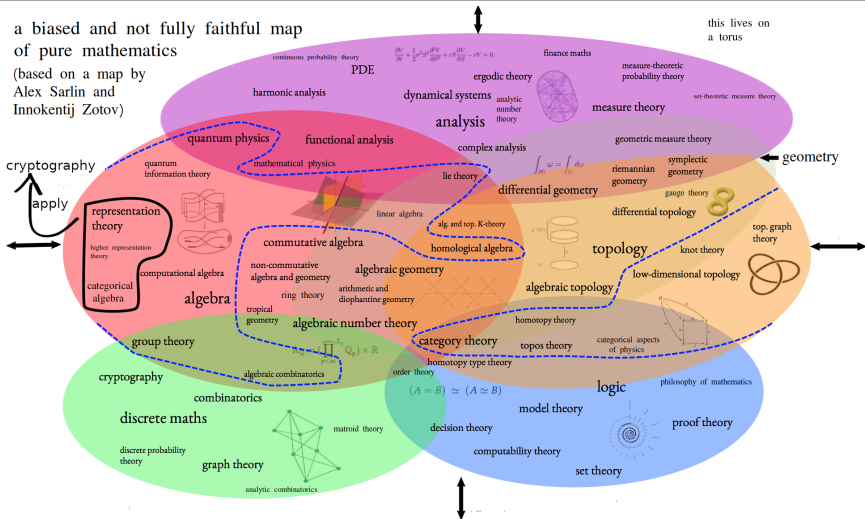
Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
$pPa_n$		YES*	$Pa_n$		YES*
$Mo_n$		YES	$RoBr_n$		YES*
$TL_n$		YES	$Br_n$		YES*
$pRo_n$		YES*	$Ro_n$		YES*
$pS_n$		EX	$S_n$		NO

Joint with Mikhail Khovanov and Maithreya Sitaraman

December 2021

# Where are we?

a biased and not fully faithful map  
of pure mathematics  
(based on a map by  
Alex Sarlin and  
Innokentij Zotov)



The six main fields of pure mathematics **algebra**, **analysis**, **geometry**, **topology**, **logic**, **discrete mathematics**

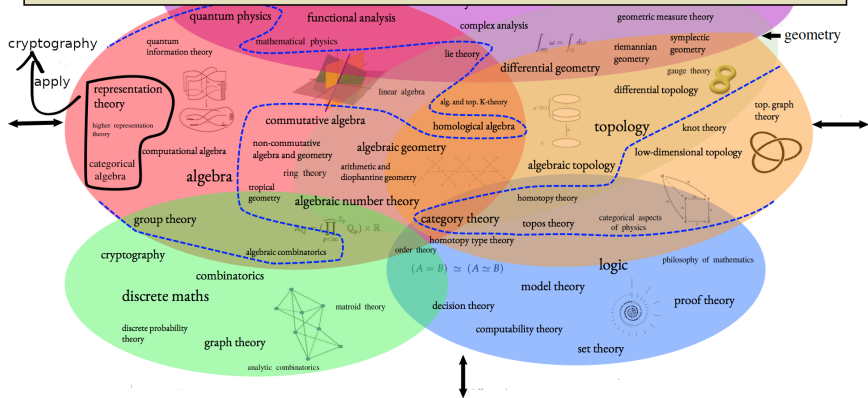
Wh

# The map of (pure) mathematics

Black box. Representation theory and its categorical analog My research area

Dashed box. Where I usually apply them My research outreach

Applications beyond my current research? The future (within NU?)



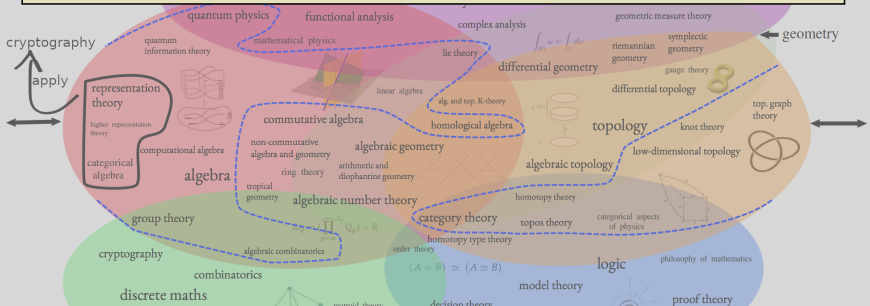
The six main fields of pure mathematics algebra, analysis, geometry, topology, logic, discrete mathematics

# The map of (pure) mathematics

Black box. Representation theory and its categorical analog My research area

Dashed box. Where I usually apply them My research outreach

Applications beyond my current research? The future (within NU?)



## Today

An applications of my work to cryptography The future (within NU?)

Why? Because it is neat (judge yourself!)  
summarizes my research areas  
and fits well to NU

# 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

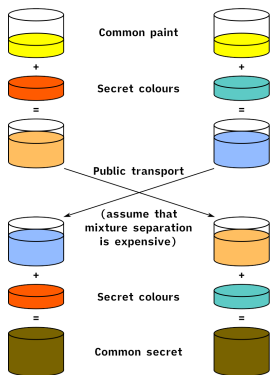


## Asymmetric encryption



- ▶ **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



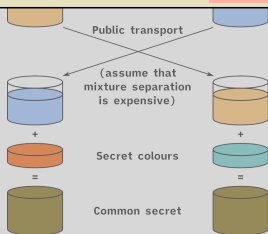
- ▶ **DH** Two secrets  $a, b$ , public  $g$ , send  $g^a$  or  $g^b$  and get  $(g^b)^a = g^{ab} = (g^a)^b$
- ▶ **Catch** Relies on the mixtures to be hard to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical ;-), so usually take  $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^\times$

## 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  $abgb'a' = baga'b'$

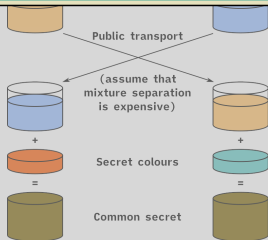
Note that  $S$  can be an arbitrary monoid in this protocol

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



- ▶ **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

**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

The representation theory group at NU knows these very well!

The good infinite examples are Artin, Thompson, Grigorchuk groups and alike

The geometric group theory group at NU knows these very well!

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

Vaguely related to the operator algebras group at NU

# Examples and non-examples

$\mathfrak{h}, G, \mathbb{F}, \ell$	Dynkin Diagrams of Simple Lie Algebras															$C_2$						
$A_1$		$A_2$		$A_3$		$A_4$		$A_5$		$A_6$		$A_7$		$A_8$		$A_9$		$A_{10}$		$C_2$		
$A_0(\mathbb{R}, \mathbb{A}_1(3))$	$A_1(3)$	$A_2(3)$	$A_3(3)$	$A_4(3)$	$A_5(3)$	$A_6(3)$	$A_7(3)$	$A_8(3)$	$A_9(3)$	$A_{10}(3)$	$A_{11}(3)$	$A_{12}(3)$	$A_{13}(3)$	$A_{14}(3)$	$A_{15}(3)$	$A_{16}(3)$	$A_{17}(3)$	$A_{18}(3)$	$A_{19}(3)$	$A_{20}(3)$	$C_3$	
60	168																				3	
$A_0(\mathbb{C}, \mathbb{B}_2(2))$	$B_2(2)$	$B_3(2)$	$B_4(2)$	$B_5(2)$	$B_6(2)$	$B_7(2)$	$B_8(2)$	$B_9(2)$	$B_{10}(2)$	$B_{11}(2)$	$B_{12}(2)$	$B_{13}(2)$	$B_{14}(2)$	$B_{15}(2)$	$B_{16}(2)$	$B_{17}(2)$	$B_{18}(2)$	$B_{19}(2)$	$B_{20}(2)$	$C_3$		
360	768																				5	
$A_7$	$A_1(11)$	$E_6(2)$	$E_7(2)$	$E_8(2)$	$F_4(2)$	$G_2(3)$	${}^3D_4(2^3)$	${}^2E_6(2^2)$	${}^2B_6(2^2)$	${}^2F_4(2)^2$	${}^2G_2(3^3)$	$B_3(2)$	$C_4(3)$	$D_5(2)$	${}^2D_5(2^2)$	${}^2A_5(25)$					$C_7$	
2520	660	231441 879333	1098000000	1098000000	3311320	4243496	231341332	76352479443	29328	17971238	30737444712	1431528	41764796	231467238	231467238	231467238	231467238	231467238	231467238	231467238	231467238	7
$A_{12}$	$A_1(13)$	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$	$G_2(4)$	${}^3D_4(3^3)$	${}^2E_6(3^2)$	${}^2B_6(3^2)$	${}^2F_4(3^2)$	${}^2G_2(3^3)$	$B_3(3)$	$C_4(3)$	$D_5(3)$	${}^2D_5(3^2)$	${}^2A_5(9)$					$C_{11}$	
30360	1892	1098000000	1098000000	1098000000	3311320	4243496	231341332	76352479443	29328	17971238	30737444712	1431528	41764796	231467238	231467238	231467238	231467238	231467238	231467238	231467238	231467238	11
$A_9$	$A_1(17)$	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$	$G_2(5)$	${}^3D_4(4^3)$	${}^2E_6(4^2)$	${}^2B_6(4^2)$	${}^2F_4(4^2)$	${}^2G_2(3^3)$	$B_3(7)$	$C_5(9)$	$D_5(3)$	${}^2D_5(3^2)$	${}^2A_5(64)$					$C_{13}$	
181440	2400	1098000000	1098000000	1098000000	3311320	4243496	231341332	76352479443	29328	17971238	30737444712	1431528	41764796	231467238	231467238	231467238	231467238	231467238	231467238	231467238	231467238	13
$A_{10}$	$A_1(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	${}^3D_4(q^3)$	${}^2E_6(q^2)$	${}^2B_6(2^{2q+1})$	${}^2F_4(q^{2q+1})$	${}^2G_2(3^{2q+1})$	$B_3(q)$	$C_6(q)$	$D_5(q)$	${}^2D_5(q^2)$	${}^2A_5(q^2)$					$C_p$	
$q$																					$p$	

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group\*
- Sporadic Groups
- Cyclic Groups

Alternating*
Cyclic**

$M_{11}$	$M_{12}$	$M_{22}$	$M_{23}$	$M_{24}$	$I_1$	$I_2$	$I_3$	$I_4$	$HS$	$McL$	$He$	$Ru$
7920	99360	443520	19200768	244320384	175360	624384	502352640	1677103360	44352000	806123040	4463367360	14072640000

\*The groups  ${}^2F_4(2)$  and  ${}^2F_4(2^2)$  are not groups of Lie type, but are sporadic groups.  ${}^2F_4(2)$  is a Suzuki group,  ${}^2F_4(2^2)$  is a Ree group.   
 \*\*The groups  ${}^2F_4(2)$  and  ${}^2F_4(2^2)$  are not groups of Lie type, but are sporadic groups.   
 \*The groups  ${}^2F_4(2)$  and  ${}^2F_4(2^2)$  are not groups of Lie type, but are sporadic groups.   
 \*\*The groups  ${}^2F_4(2)$  and  ${}^2F_4(2^2)$  are not groups of Lie type, but are sporadic groups.   
 Copyright © 2004 Tom Bruhin

$S_2$	$Suz_2$	${}^2F_4(2)$	${}^2F_4(2^2)$	${}^2F_4(2^4)$	${}^2F_4(2^8)$	${}^2F_4(2^{16})$	${}^2F_4(2^{32})$	${}^2F_4(2^{64})$	${}^2F_4(2^{128})$	${}^2F_4(2^{256})$	${}^2F_4(2^{512})$	${}^2F_4(2^{1024})$
6	20160	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000	1098000000

- ▶ 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 the named ones

$A_0$	$A_1$	$A_2$	$A_3$	$A_4$	$A_5$	$A_6$	$A_7$	$A_8$	$A_9$	$A_{10}$
1	2	3	4	5	6	7	8	9	10	11
1	3	6	10	15	21	28	36	45	55	66
1	1	1	1	1	1	1	1	1	1	1

■ Alternating  
■ Classical  
■ Classical  
■ Steinberg  
■ Suzuki  
■ Ree  
■ Sporadic  
■ Cyclic

\*The 26 groups  ${}^2F_4(q)$  are not a group of Lie type, but do form a disconnected subgroup of  ${}^2F_4(q)$ . It is usually given because Lie type groups.

\*The group  ${}^2G_2(3)$  is not a group of Lie type, but it is closely related to the classical groups. The groups  ${}^2G_2(3)$  and  ${}^2G_2(9)$  are not simple groups, but are closely related to the simple groups.

\*The group  ${}^2G_2(3)$  is not a group of Lie type, but it is closely related to the classical groups. The groups  ${}^2G_2(3)$  and  ${}^2G_2(9)$  are not simple groups, but are closely related to the simple groups.

Copyright © 2008 Tom Ruch

Dynkin Diagrams of Simple Lie Algebras

$A_n$

$B_n$

$C_n$

$D_n$

$E_6$

$E_7$

$E_8$

$F_4$

$G_2$

$H_3$

$I_2(n)$

${}^2A_1(3)$	$A_1(2)$	$A_2(3)$	$A_3(4)$	$A_4(5)$	$A_5(6)$	$A_6(7)$	$A_7(8)$	$A_8(9)$	$A_9(10)$	$A_{10}(11)$	$C_2$
1	2	3	4	5	6	7	8	9	10	11	2
1	2	3	4	5	6	7	8	9	10	11	2

$S_3$	${}^2F_4(3)$	${}^2F_4(4)$	${}^2F_4(5)$	${}^2F_4(7)$	${}^2F_4(8)$	${}^2F_4(9)$	${}^2F_4(11)$	${}^2F_4(13)$	${}^2F_4(16)$	${}^2F_4(17)$	${}^2F_4(19)$	${}^2F_4(23)$	${}^2F_4(25)$	${}^2F_4(29)$	${}^2F_4(31)$	${}^2F_4(37)$	${}^2F_4(41)$	${}^2F_4(47)$	${}^2F_4(53)$	${}^2F_4(59)$	${}^2F_4(71)$	${}^2F_4(73)$	${}^2F_4(79)$	${}^2F_4(83)$	${}^2F_4(97)$	${}^2F_4(103)$	${}^2F_4(107)$	${}^2F_4(113)$	${}^2F_4(127)$	${}^2F_4(131)$	${}^2F_4(137)$	${}^2F_4(139)$	${}^2F_4(143)$	${}^2F_4(149)$	${}^2F_4(151)$	${}^2F_4(157)$	${}^2F_4(163)$	${}^2F_4(167)$	${}^2F_4(173)$	${}^2F_4(179)$	${}^2F_4(181)$	${}^2F_4(187)$	${}^2F_4(191)$	${}^2F_4(193)$	${}^2F_4(199)$	${}^2F_4(211)$	${}^2F_4(217)$	${}^2F_4(223)$	${}^2F_4(227)$	${}^2F_4(229)$	${}^2F_4(233)$	${}^2F_4(239)$	${}^2F_4(241)$	${}^2F_4(247)$	${}^2F_4(251)$	${}^2F_4(257)$	${}^2F_4(263)$	${}^2F_4(269)$	${}^2F_4(271)$	${}^2F_4(277)$	${}^2F_4(281)$	${}^2F_4(283)$	${}^2F_4(287)$	${}^2F_4(293)$	${}^2F_4(299)$	${}^2F_4(307)$	${}^2F_4(311)$	${}^2F_4(313)$	${}^2F_4(317)$	${}^2F_4(323)$	${}^2F_4(329)$	${}^2F_4(331)$	${}^2F_4(337)$	${}^2F_4(347)$	${}^2F_4(349)$	${}^2F_4(353)$	${}^2F_4(359)$	${}^2F_4(367)$	${}^2F_4(373)$	${}^2F_4(379)$	${}^2F_4(383)$	${}^2F_4(389)$	${}^2F_4(397)$	${}^2F_4(401)$	${}^2F_4(407)$	${}^2F_4(413)$	${}^2F_4(419)$	${}^2F_4(421)$	${}^2F_4(427)$	${}^2F_4(431)$	${}^2F_4(433)$	${}^2F_4(437)$	${}^2F_4(443)$	${}^2F_4(449)$	${}^2F_4(457)$	${}^2F_4(461)$	${}^2F_4(463)$	${}^2F_4(467)$	${}^2F_4(473)$	${}^2F_4(479)$	${}^2F_4(481)$	${}^2F_4(487)$	${}^2F_4(491)$	${}^2F_4(493)$	${}^2F_4(499)$	${}^2F_4(503)$	${}^2F_4(509)$	${}^2F_4(511)$	${}^2F_4(517)$	${}^2F_4(521)$	${}^2F_4(523)$	${}^2F_4(527)$	${}^2F_4(533)$	${}^2F_4(539)$	${}^2F_4(541)$	${}^2F_4(547)$	${}^2F_4(551)$	${}^2F_4(557)$	${}^2F_4(563)$	${}^2F_4(569)$	${}^2F_4(571)$	${}^2F_4(577)$	${}^2F_4(581)$	${}^2F_4(583)$	${}^2F_4(587)$	${}^2F_4(593)$	${}^2F_4(599)$	${}^2F_4(601)$	${}^2F_4(607)$	${}^2F_4(611)$	${}^2F_4(613)$	${}^2F_4(617)$	${}^2F_4(619)$	${}^2F_4(623)$	${}^2F_4(629)$	${}^2F_4(631)$	${}^2F_4(637)$	${}^2F_4(641)$	${}^2F_4(643)$	${}^2F_4(647)$	${}^2F_4(653)$	${}^2F_4(659)$	${}^2F_4(661)$	${}^2F_4(667)$	${}^2F_4(671)$	${}^2F_4(673)$	${}^2F_4(677)$	${}^2F_4(683)$	${}^2F_4(689)$	${}^2F_4(691)$	${}^2F_4(697)$	${}^2F_4(701)$	${}^2F_4(703)$	${}^2F_4(707)$	${}^2F_4(713)$	${}^2F_4(719)$	${}^2F_4(721)$	${}^2F_4(727)$	${}^2F_4(731)$	${}^2F_4(733)$	${}^2F_4(737)$	${}^2F_4(743)$	${}^2F_4(749)$	${}^2F_4(751)$	${}^2F_4(757)$	${}^2F_4(761)$	${}^2F_4(763)$	${}^2F_4(767)$	${}^2F_4(773)$	${}^2F_4(779)$	${}^2F_4(781)$	${}^2F_4(787)$	${}^2F_4(791)$	${}^2F_4(793)$	${}^2F_4(799)$	${}^2F_4(803)$	${}^2F_4(809)$	${}^2F_4(811)$	${}^2F_4(817)$	${}^2F_4(821)$	${}^2F_4(823)$	${}^2F_4(827)$	${}^2F_4(833)$	${}^2F_4(839)$	${}^2F_4(841)$	${}^2F_4(847)$	${}^2F_4(851)$	${}^2F_4(853)$	${}^2F_4(857)$	${}^2F_4(859)$	${}^2F_4(863)$	${}^2F_4(869)$	${}^2F_4(871)$	${}^2F_4(877)$	${}^2F_4(881)$	${}^2F_4(883)$	${}^2F_4(887)$	${}^2F_4(893)$	${}^2F_4(899)$	${}^2F_4(901)$	${}^2F_4(907)$	${}^2F_4(911)$	${}^2F_4(913)$	${}^2F_4(917)$	${}^2F_4(919)$	${}^2F_4(923)$	${}^2F_4(929)$	${}^2F_4(931)$	${}^2F_4(937)$	${}^2F_4(941)$	${}^2F_4(943)$	${}^2F_4(947)$	${}^2F_4(953)$	${}^2F_4(959)$	${}^2F_4(961)$	${}^2F_4(967)$	${}^2F_4(971)$	${}^2F_4(973)$	${}^2F_4(977)$	${}^2F_4(983)$	${}^2F_4(989)$	${}^2F_4(991)$	${}^2F_4(997)$
-------	--------------	--------------	--------------	--------------	--------------	--------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	---------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------

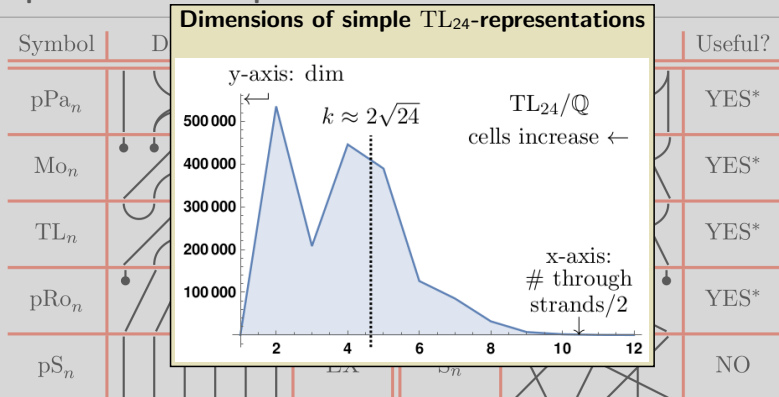
- Classical examples   Cyclic groups have only big representations over  $\mathbb{F}_p$
- Non-examples   Groups of Lie type have all very small representations
- Non-examples   Sporadic groups are too small to be useful

## 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 and geometric group theory will also work - lets work on this at NU!

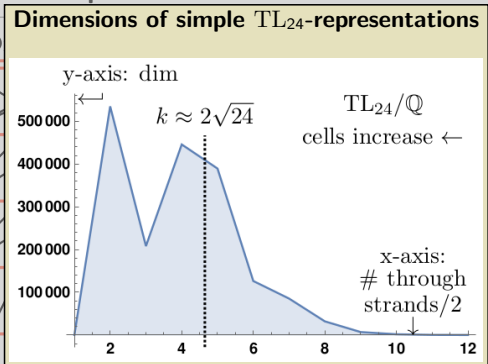
## Examples and non-examples



- ▶ **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 and geometric group theory will also work - lets work on this at NU!

# Examples and non-examples

Symbol	D	Useful?
$pPa_n$		YES*
$Mo_n$		YES*
$TL_n$		YES*
$pRo_n$		YES*
$pS_n$		NO



## Example (following Spencer ~2021)

After appropriate truncation

the representation gap of  $TL_n$  is bounded from below by

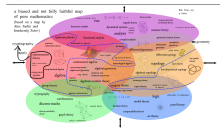
$$\frac{4}{(n + \lfloor 2\sqrt{n} \rfloor + 2)(n + \lfloor 2\sqrt{n} \rfloor + 4)} \binom{n}{(\lfloor 2\sqrt{n} \rfloor)/2}$$

topology and

geometric group theory will also work - lets work on this at NU!



## Where are we?



The six main fields of pure mathematics: **algebra**, **analysis**, **geometry**, **topology**, **logic**, **discrete mathematics**.

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## 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** Rules on the mixtures to be hard to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical  $\rightarrow$ , so usually take  $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^*$

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$\mu\mathbb{P}_n$		YES	$\mathbb{P}_n$		YES
$M_n$		YES	$B_n$		YES
$TL_n$		YES	$B_n$		YES
$\mu\mathbb{B}_n$		YES	$B_n$		YES
$\mu\mathbb{S}_n$		EX	$\mathbb{S}_n$		NO

- ▶ **Classical example** 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 Diagrammatics and cryptography November 2021 5/5

## End-to-end encryption



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

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## 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 (Miyahara-Gishaku (SU) key exchange protocol)**

The public data is a monoid  $S$ , and two sets  $A, B \subseteq S$  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  $gbg'$  and the common secret is  $agb'a' = ag'a'b$ .

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.

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$\mu\mathbb{P}_n$		YES	$\mathbb{P}_n$		YES
$M_n$		YES	$B_n$		YES
$TL_n$		YES	$B_n$		YES
$\mu\mathbb{B}_n$		YES	$B_n$		YES
$\mu\mathbb{S}_n$		EX	$\mathbb{S}_n$		NO

- ▶ **New examples** Finite monoids coming from quantum topology
- ▶ **More specific** Submonoids of the partition monoid above
- ▶ **Complexity open** I claim your favorite example from quantum topology and geometric group theory will also work - lets work on this at NU!

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## End-to-end 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

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## End-to-end encryption

**Linear attack (Miyahara-Roman'kov - 2015)**

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

**Enter representation theory**

**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

**The representation theory group at NU knows these very well!**

The good infinite examples are Artin, Thompson, Garguchuk groups and allies

**The geometric group theory group at NU knows these very well!**

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

**Vaguely related to the operator algebras group at NU!**

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

## Examples and non-examples

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

Symbol:  $\mu\mathbb{P}_n$ ,  $M_n$ ,  $TL_n$ ,  $\mu\mathbb{B}_n$ ,  $\mu\mathbb{S}_n$

Diagram:

Useful?: YES, YES, YES, YES, NO

Symbol:  $\mathbb{P}_n$ ,  $B_n$ ,  $B_n$ ,  $B_n$ ,  $\mathbb{S}_n$

Diagram:

Useful?: YES, YES, YES, YES, NO

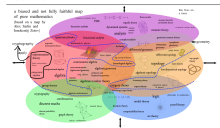
Graph:

- ▶ **New example** After appropriate truncation the representation gap of  $TL_n$  is bounded from below by  $\frac{1}{2} \sqrt{2n-1}$
- ▶ **More specific**  $\mathbb{P}_n$  and  $B_n$  are the only monoids with no small non-trivial representations
- ▶ **Complexity open** I claim your favorite example from quantum topology and geometric group theory will also work - lets work on this at NU!

David Tubbenhauer Diagrammatics and cryptography November 2021 5/5

There is still much to do...

### Where are we?



The six main fields of pure mathematics: **algebra**, **analysis**, **geometry**, **topology**, **logic**, **discrete mathematics**.

### 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** Rules on the mixtures to be hard to decompose (discrete log problem)
- ▶ **BTW** Using colors is not very practical  $\rightarrow$ , so usually take  $a, b, g \in (\mathbb{Z}/p\mathbb{Z})^*$

### Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$\mu\mathbb{P}_n$		YES	$\mathbb{P}_n$		YES
$M_n$		YES	$B_n$		YES
$TL_n$		YES	$B_n$		YES
$\mu\mathbb{P}_n$		YES	$B_n$		YES
$\mu\mathbb{S}_n$		EX	$S_n$		NO

- ▶ **Classical example** 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

### End-to-end encryption



- ▶ **CRUE** 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



**Example (Sylvestre-Gibson (SG) key exchange protocol)**

The public data is a monoid  $S$ , and two sets  $A, B \subseteq S$  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  $gbg'$  and the common secret is  $agb'a' = agb'a'$

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.

### Examples and non-examples

Symbol	Diagram	Useful?	Symbol	Diagram	Useful?
$\mu\mathbb{P}_n$		YES	$\mathbb{P}_n$		YES
$M_n$		YES	$B_n$		YES
$TL_n$		YES	$B_n$		YES
$\mu\mathbb{P}_n$		YES	$B_n$		YES
$\mu\mathbb{S}_n$		EX	$S_n$		NO

- ▶ **New examples** Finite monoids coming from quantum topology
- ▶ **More specific** Submonoids of the partition monoid above
- ▶ **Complexity open** I claim your favorite example from quantum topology and geometric group theory will also work - lets work on this at NU!

### End-to-end 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



**Enter representation theory**

**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

The good infinite examples are Artin, Thompson, Garguchuk groups and allies

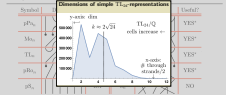
The representation theory group at NU knows these very well!

The geometric group theory group at NU knows these very well!

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

Vaguely related to the operator algebra group at NU!

### Examples and non-examples



- ▶ **Example (following Spencer - 2021)**
- ▶ **New class** After appropriate truncation the representation gap of  $TL_n$  is bounded from below by  $\frac{1}{2}n^{3/2}$
- ▶ **More specific**  $\mathbb{Z}/2\mathbb{Z}$  and  $\mathbb{Z}/3\mathbb{Z}$
- ▶ **Complexity open** I claim your favorite example from quantum topology and geometric group theory will also work - lets work on this at NU!

Thanks for your attention!