v.20231123

Hacking a magnetic lock: successes and failures

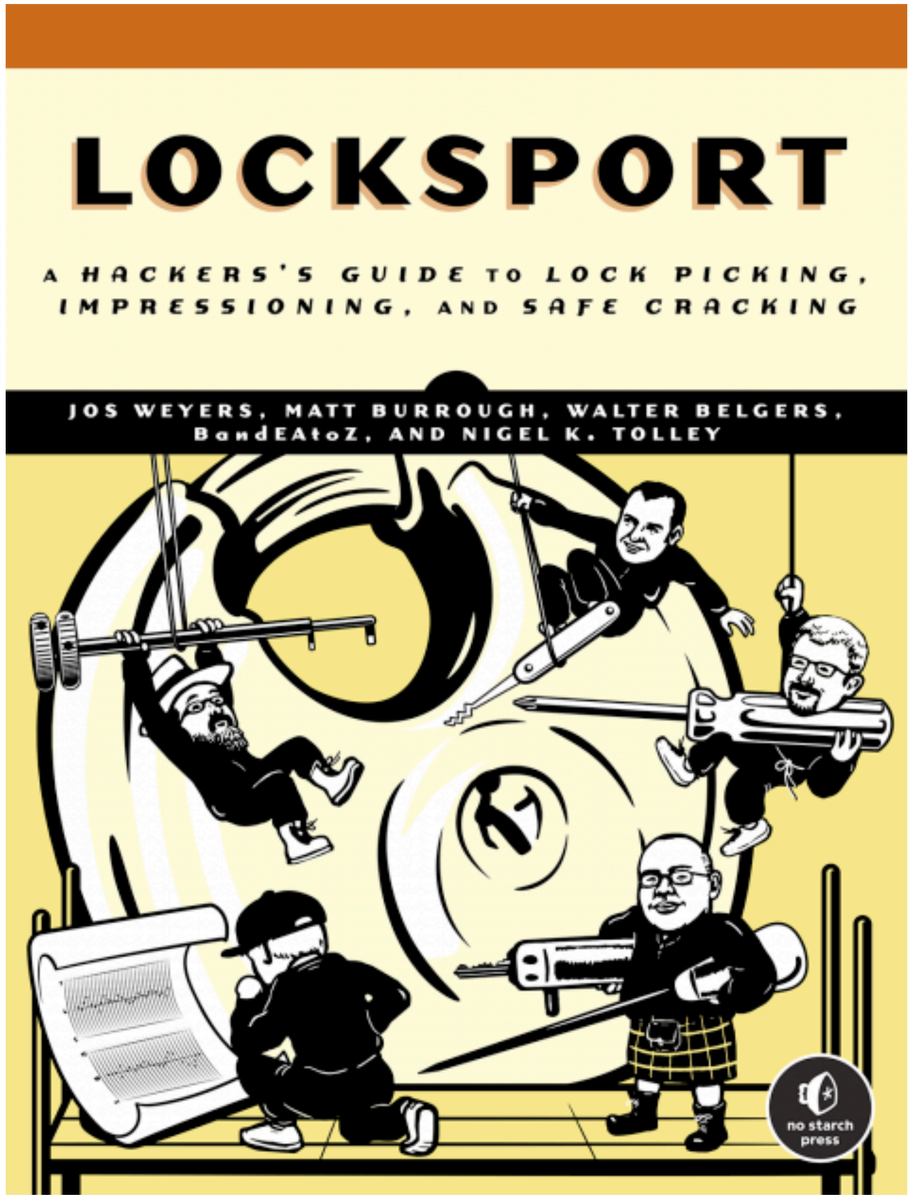
Walter Belgers
/wɑːltəR bælɣəRs/
walter@belge.rs

DefCamp#8
Where Hacking & Security Collide

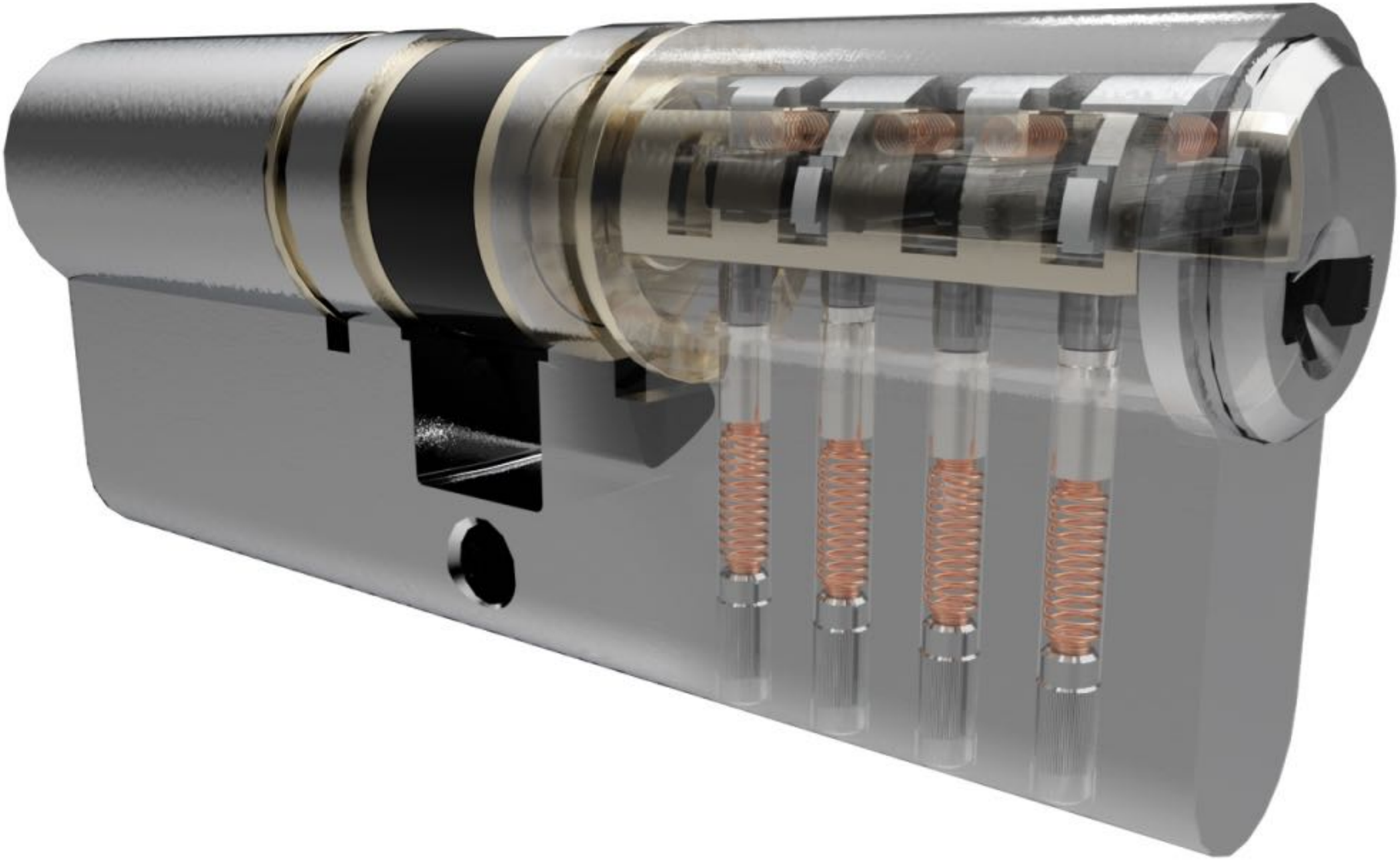
MIWA/Anker 3800

TOOOL

The Open Organisation Of Lockpickers



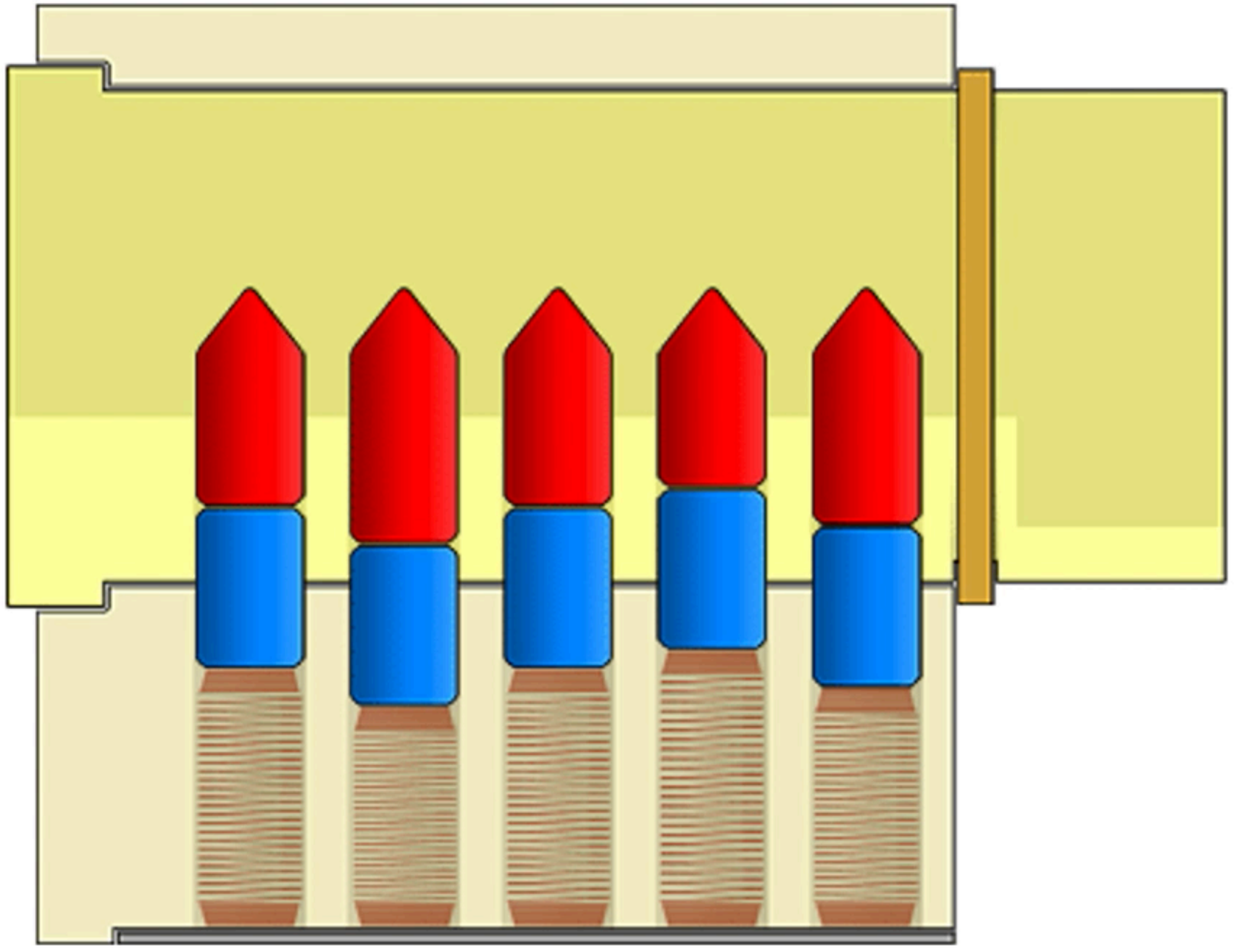
https://nostarch.com/locksport



Bottom: 4 pins, 4 possible depths

Top: 4 sets of 2 Samarium-Cobalt magnets or fakes, 2x2mm, moving 4 sliders

Four pins



Four sliders

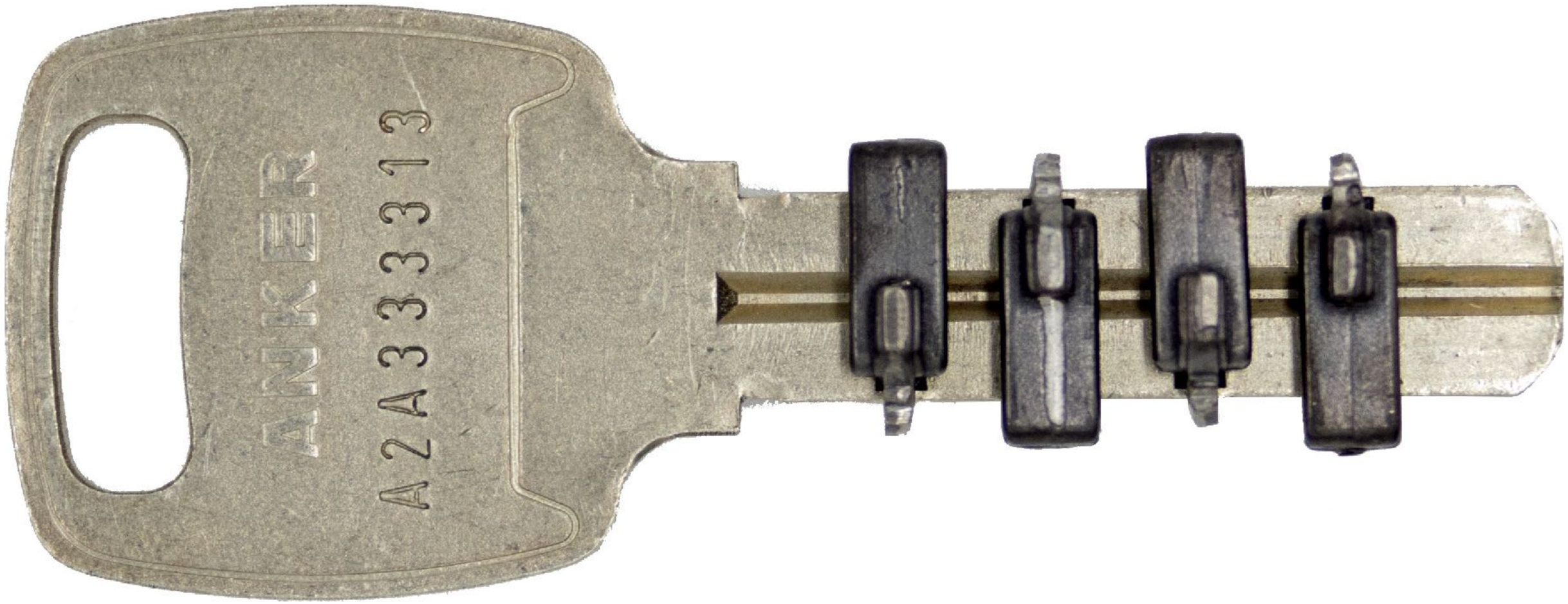


Photo shop
ACHIEVEMENT
UNLOCKED

FIG. 3

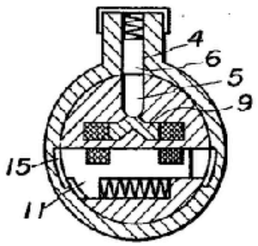
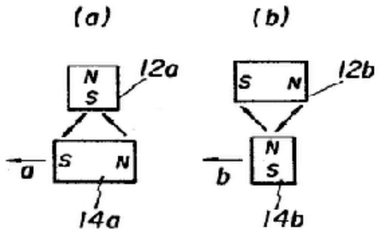
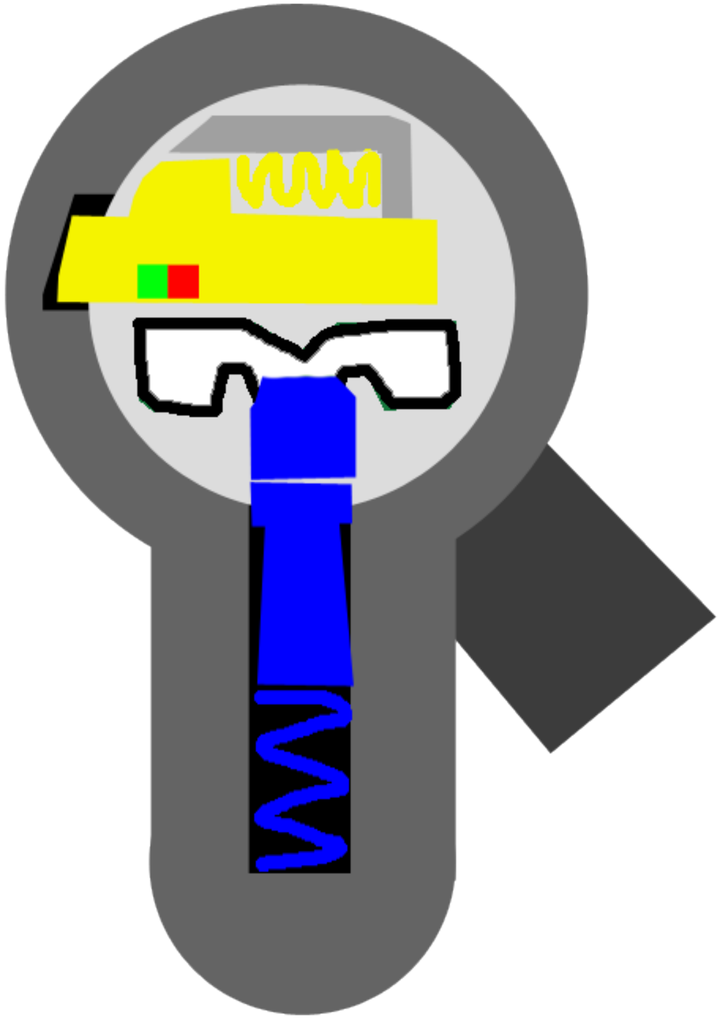
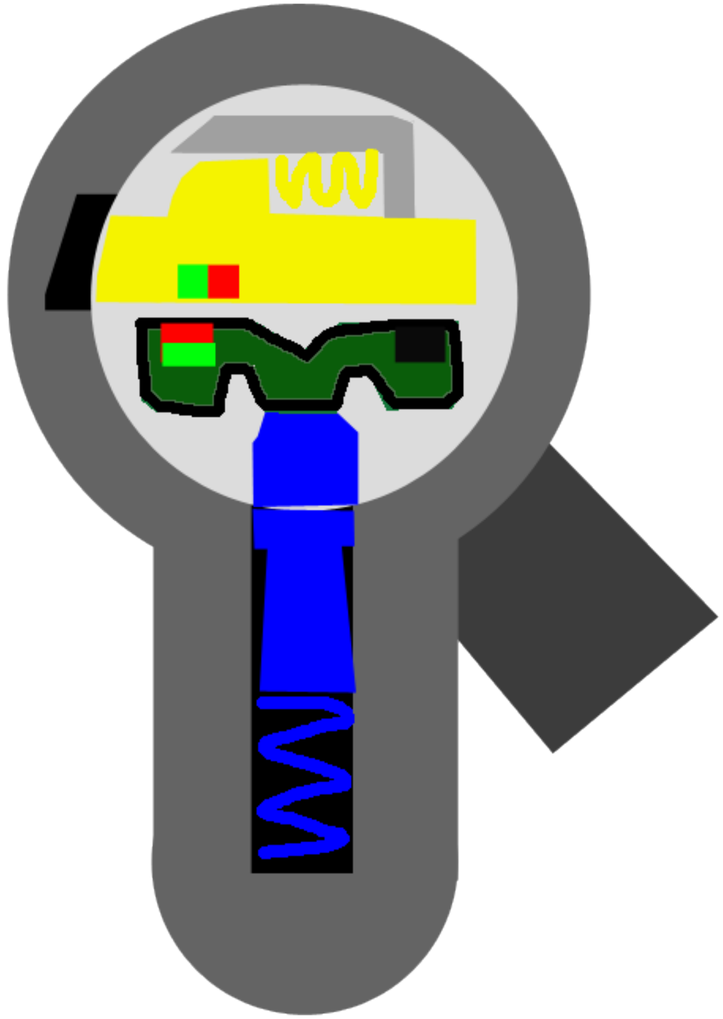

4
6
5
9
15
11

FIG. 4

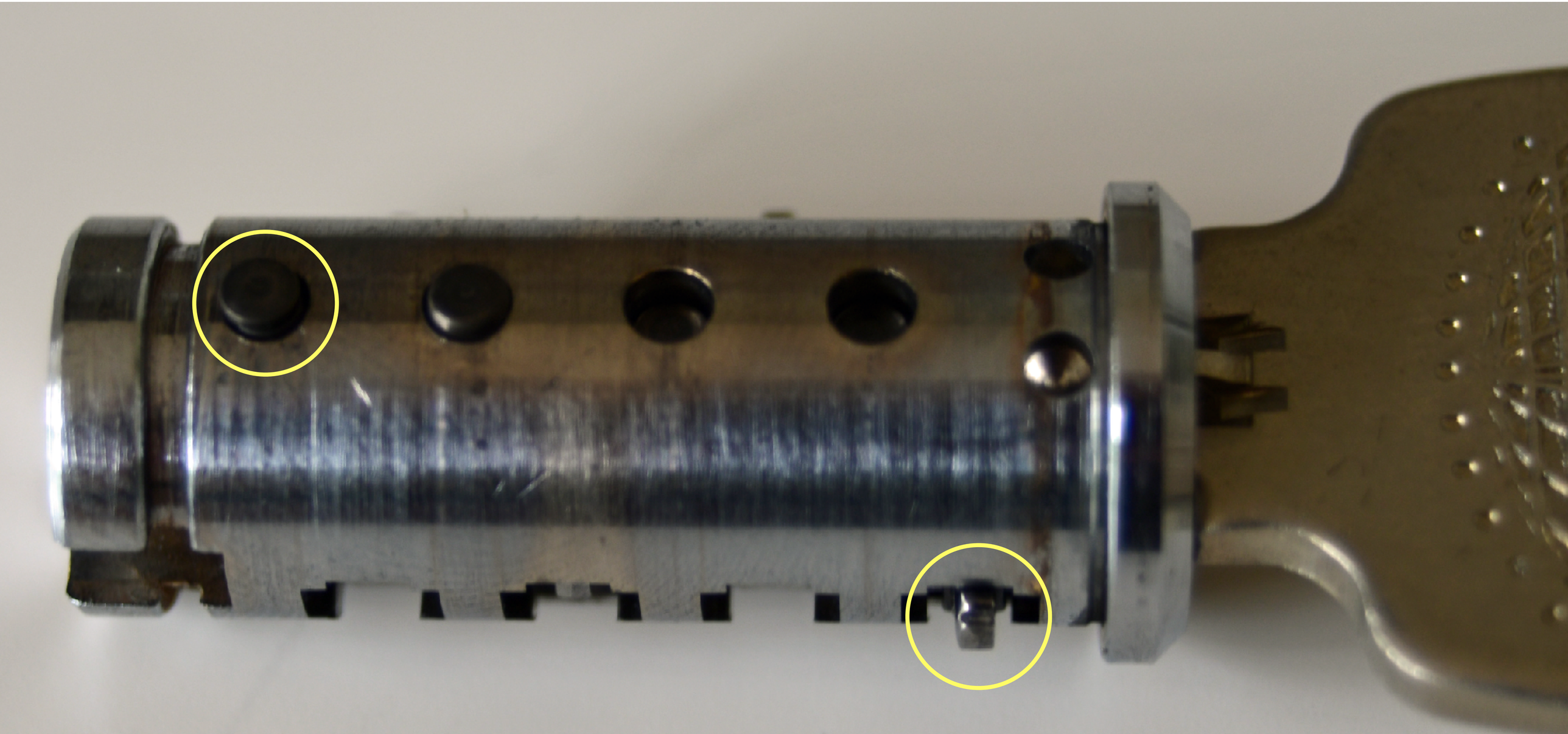

(a)
(b)
N
S
12a
S
N
12b
a
S
N
b
N
S
14a
14b



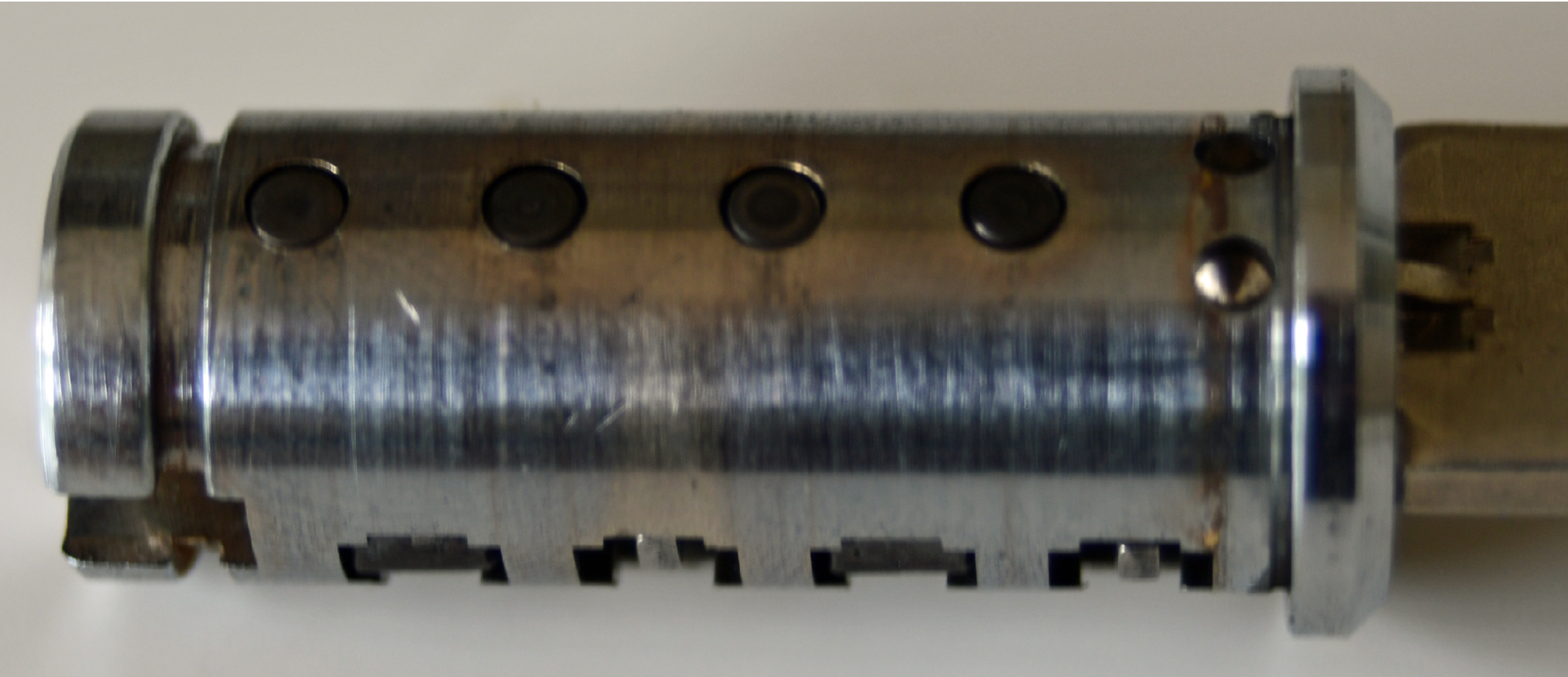


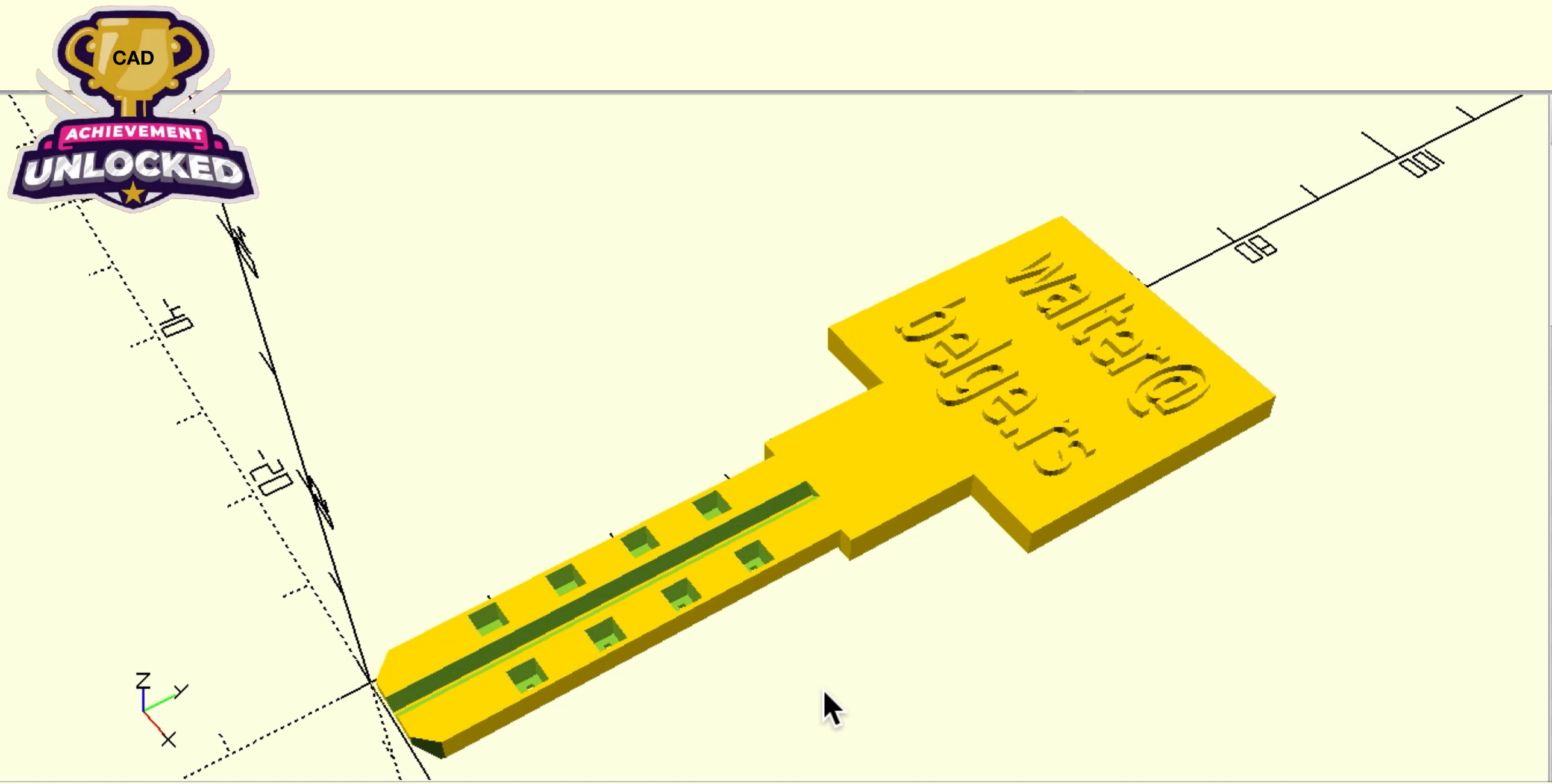
Key magnets

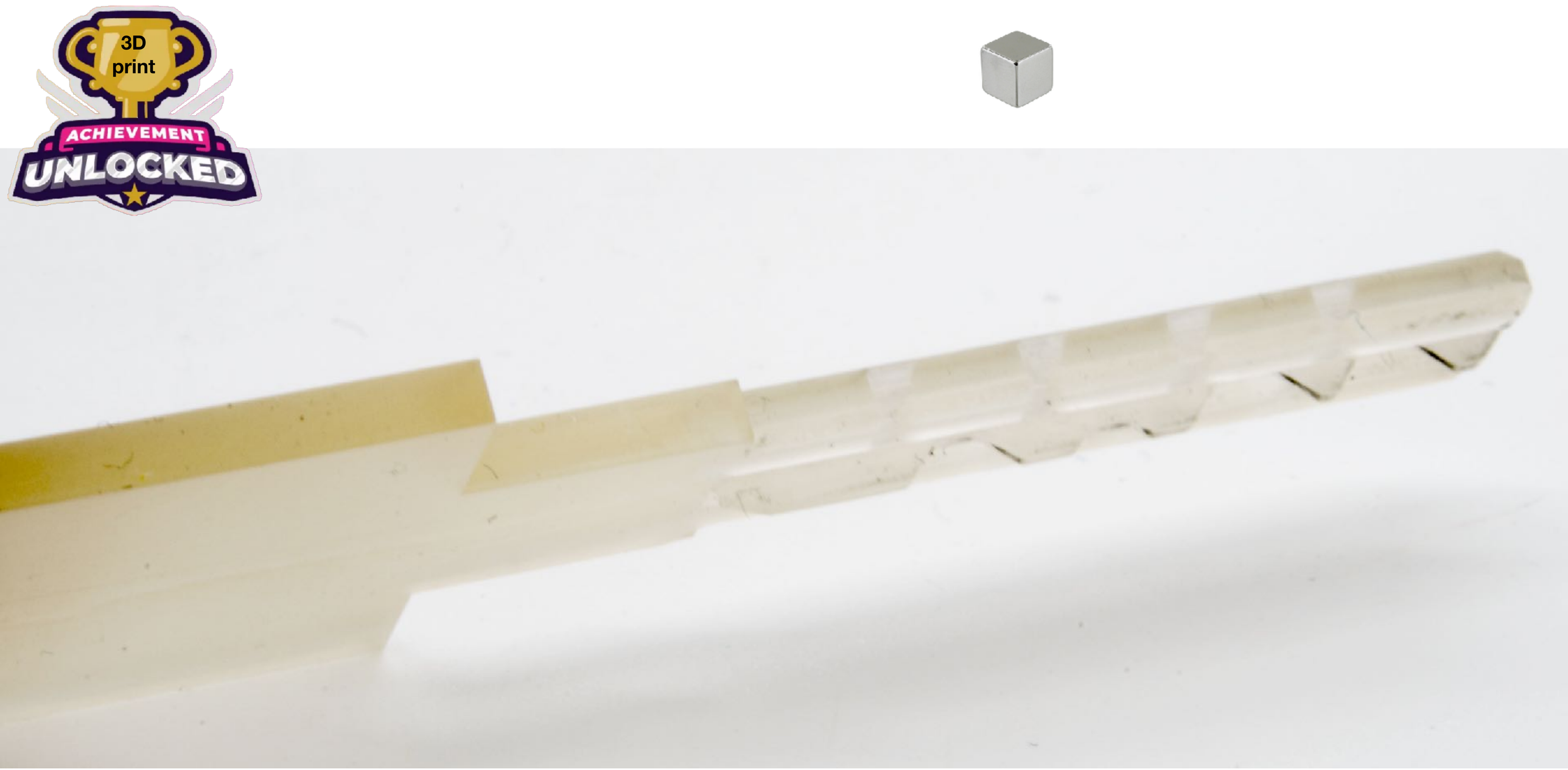
Incorrect key

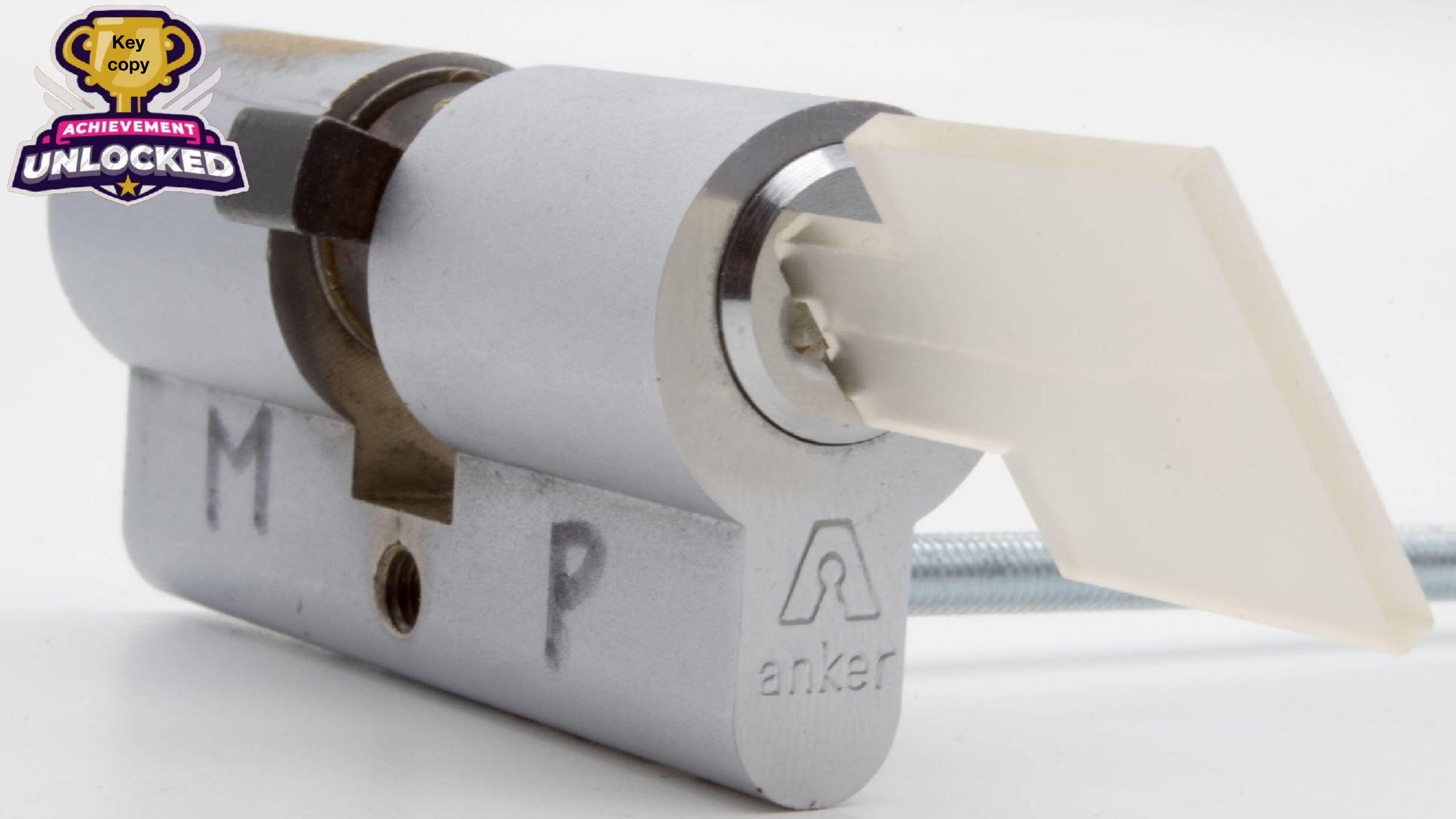


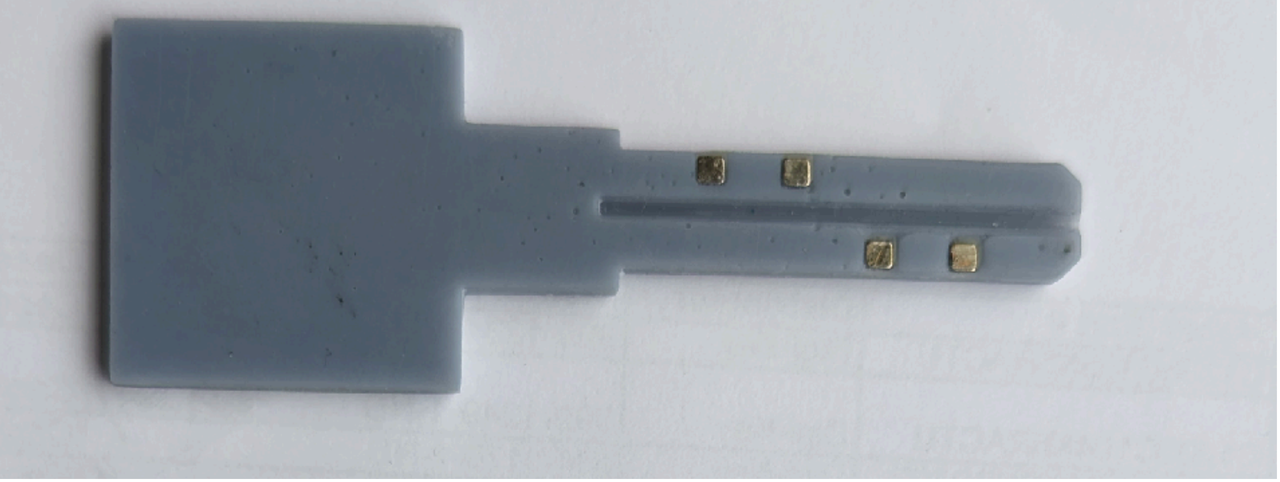
Correct key




CAD
ACHIEVEMENT
UNLOCKED
walter@
delgado
Z
Y
X


3D
print
ACHIEVEMENT
UNLOCKED


Key copy
ACHIEVEMENT
UNLOCKED
M
P
anker



2x2x2mm

1x1x1mm

Too small

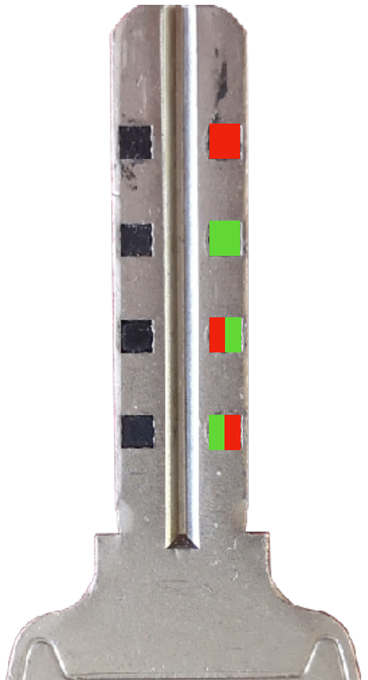
2x1mm

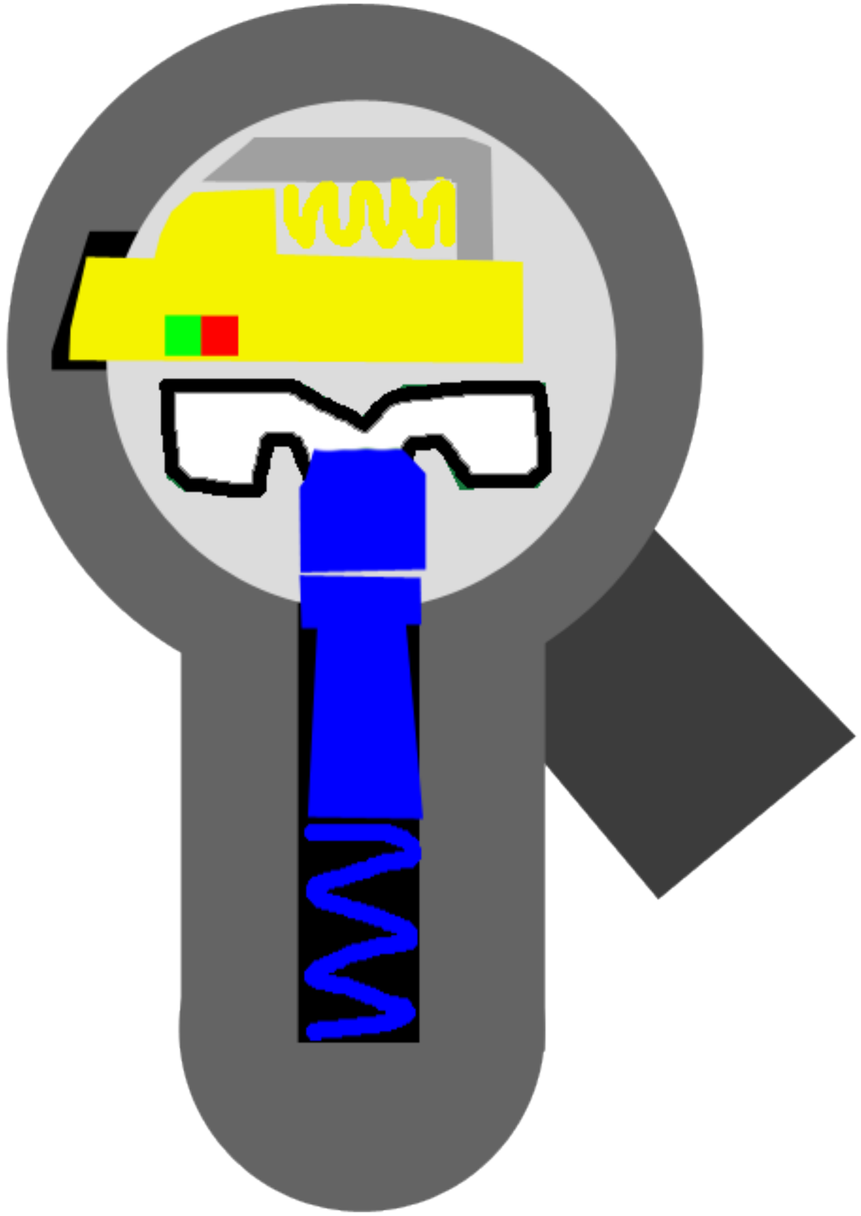
Attack vector

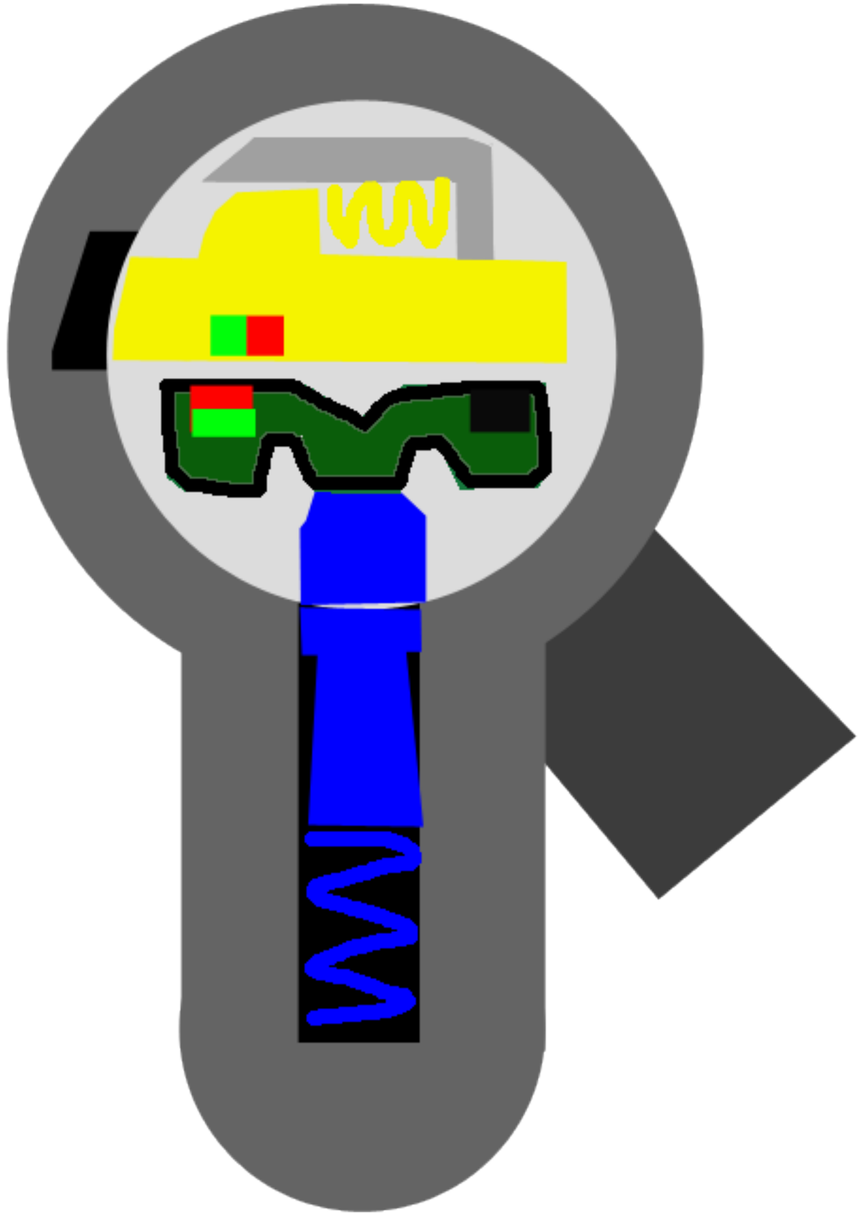
- When you have (temporary) access to the key, it can be copied
  - Read out the pin heights with the naked eye
  - Read out the magnets with a magnetometer
  - Print a duplicate key and insert correct magnets

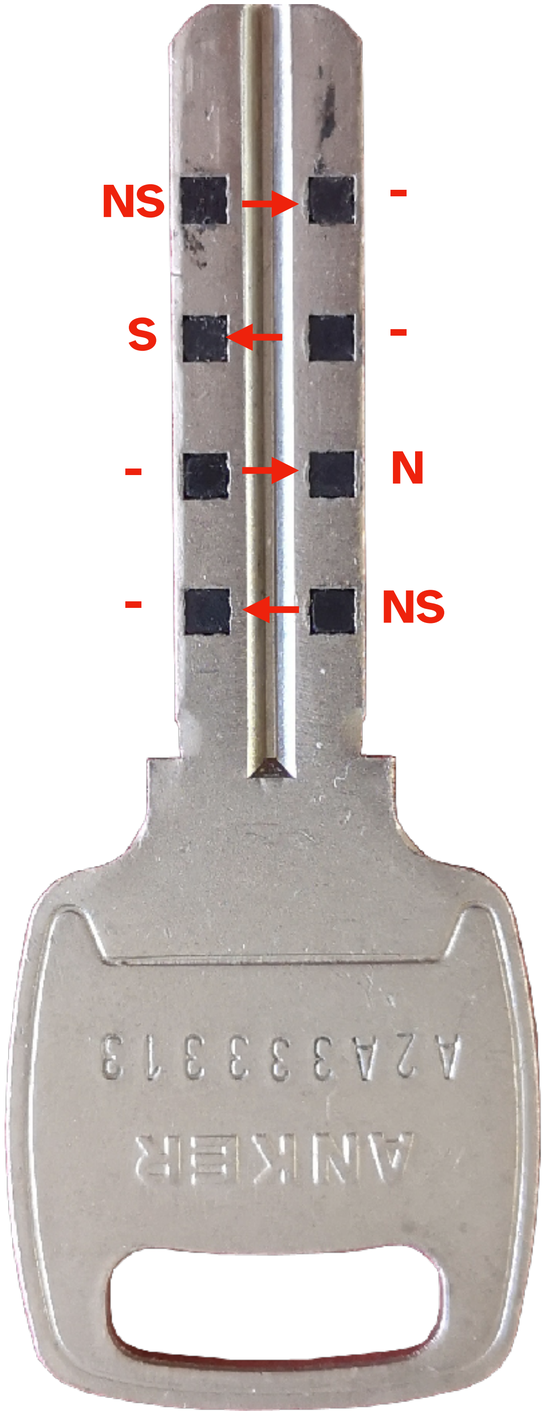
From key to cylinder

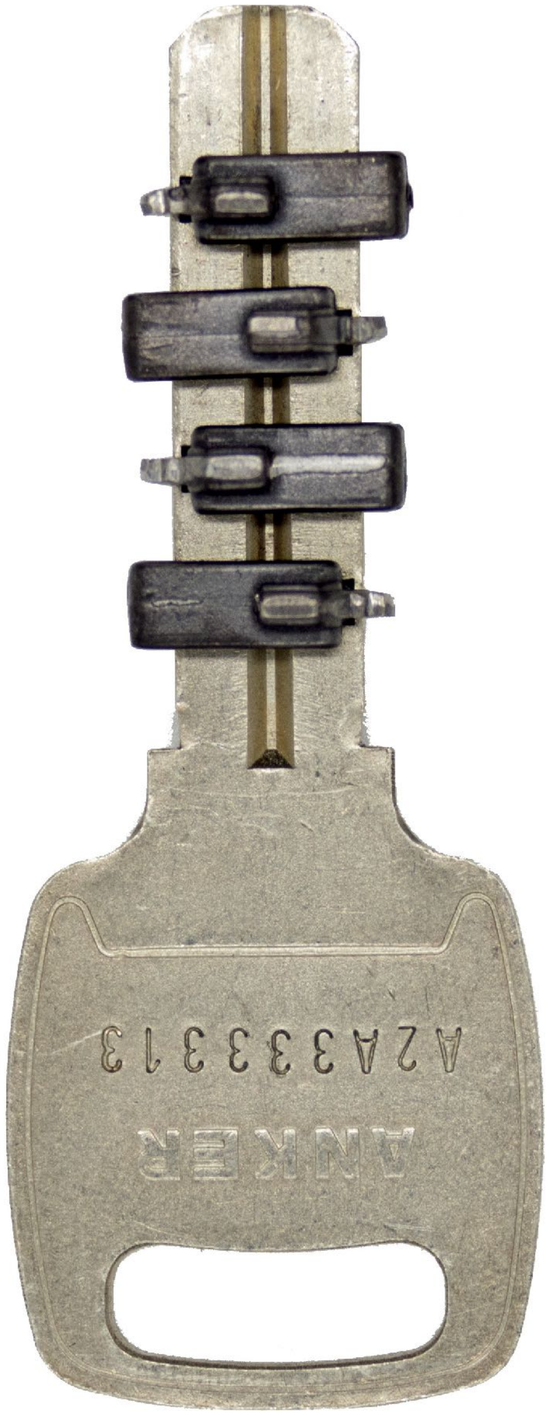
And vice versa

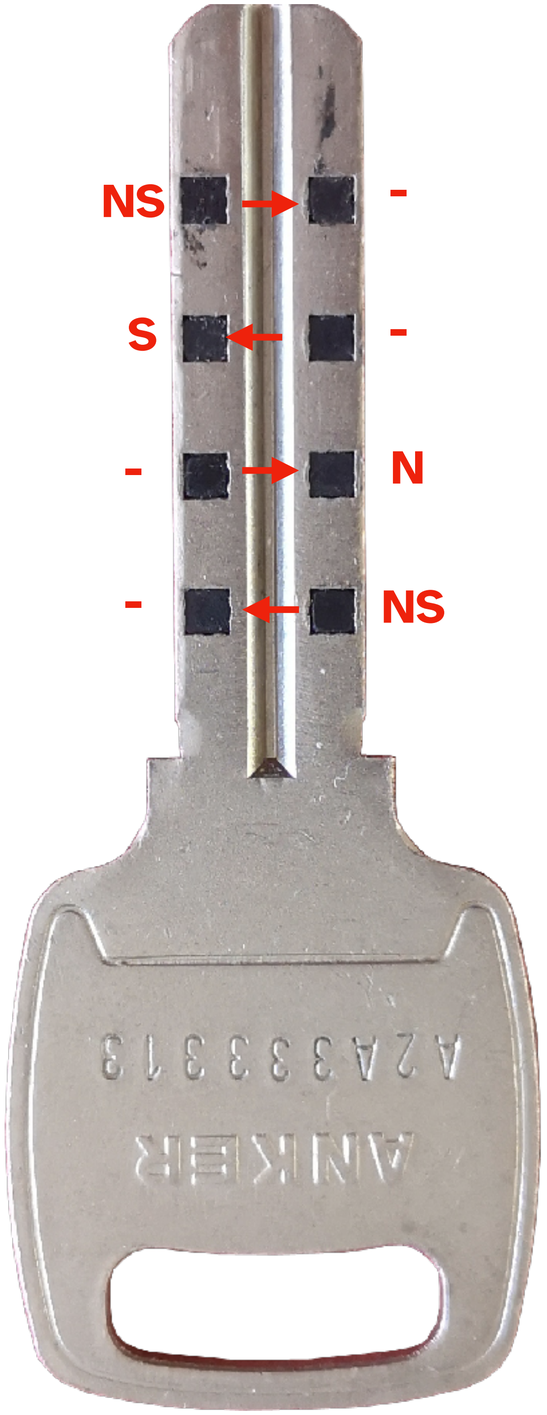


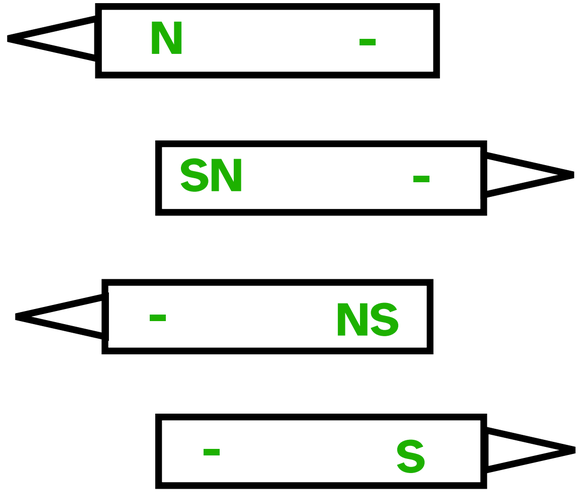


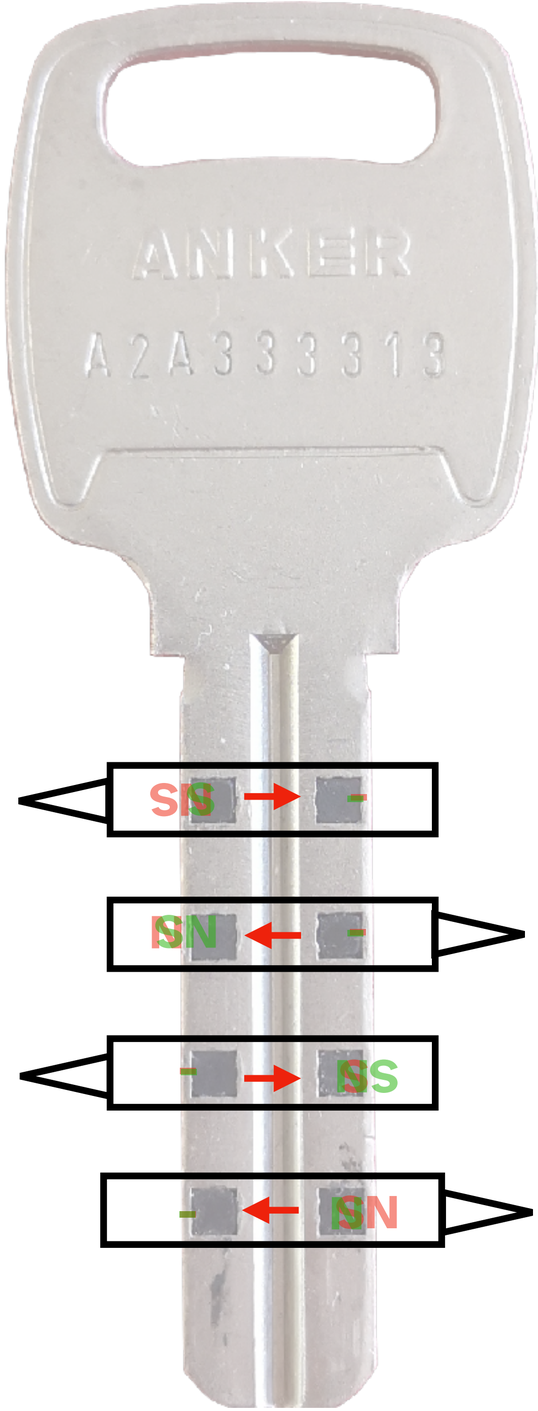


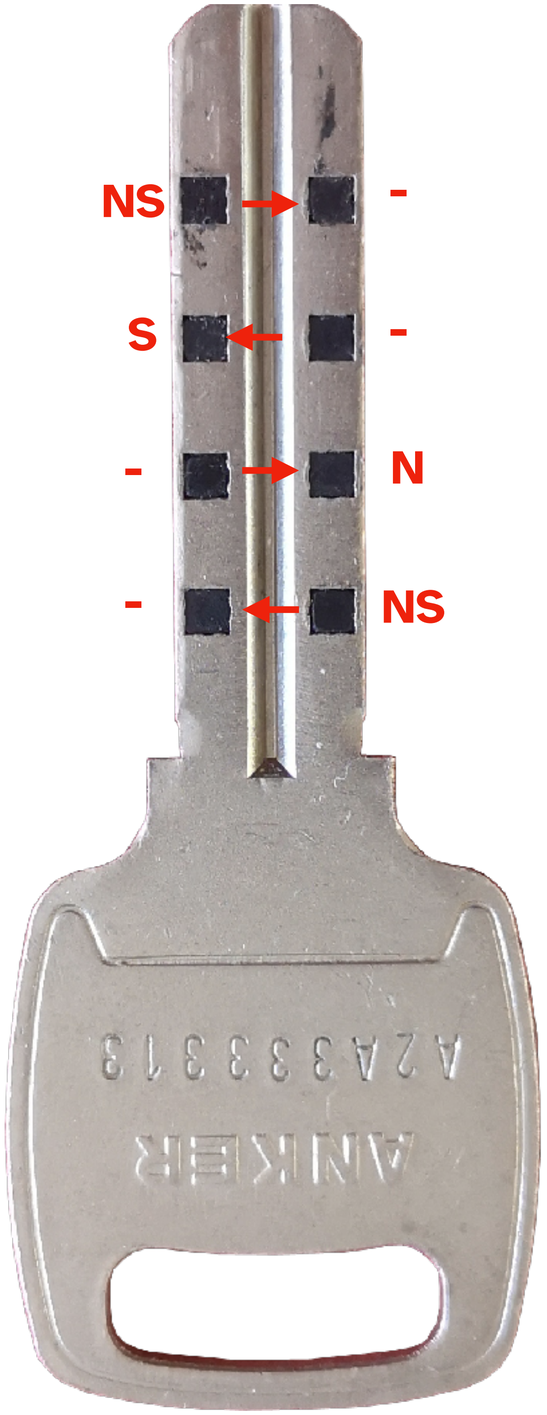

NS
-
S
-
-
N
-
NS
A2A33313
ANKER

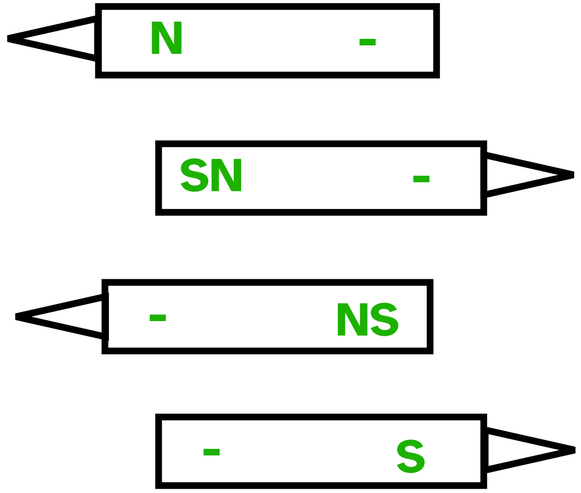

A2A33313
ANKER


NS
-
S
-
-
N
-
NS
ANKER
A2A33313


N -
SN -
- NS
- S


ANKER
A2A333313
SS
SN
SS
SN

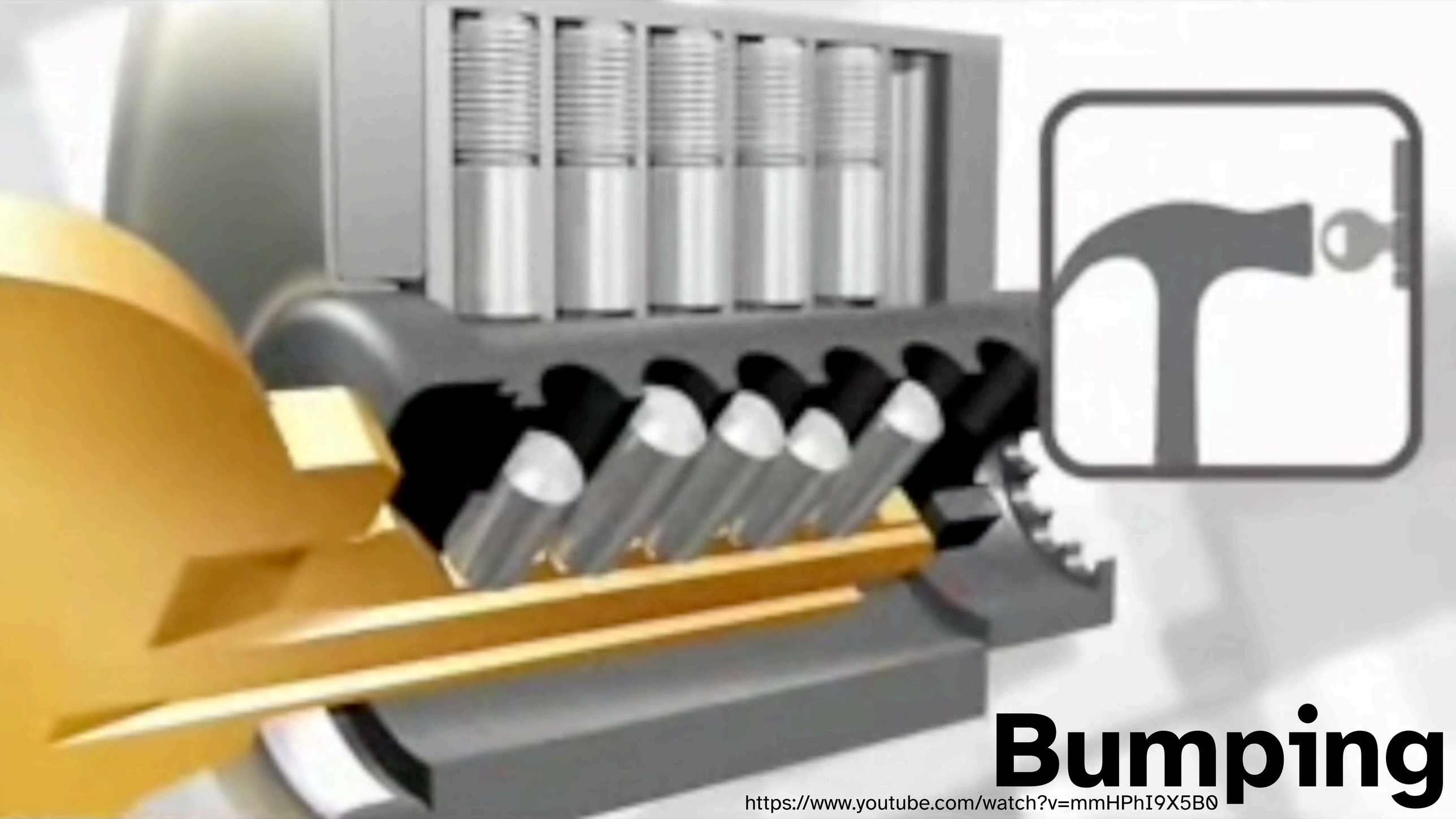

NS
-
S
-
-
N
-
NS
ANKER
A2A33313


N -
SN -
- NS
- S

Ardu
ino
ACHIEVEMENT
UNLOCKED

Attack vector

- When you have (temporary) access to the cylinder but not to its key
  - Read out magnets from the cylinder, determine magnets that should be in the key
  - What about pins? Try 4*4*4*4=256 possible keys?

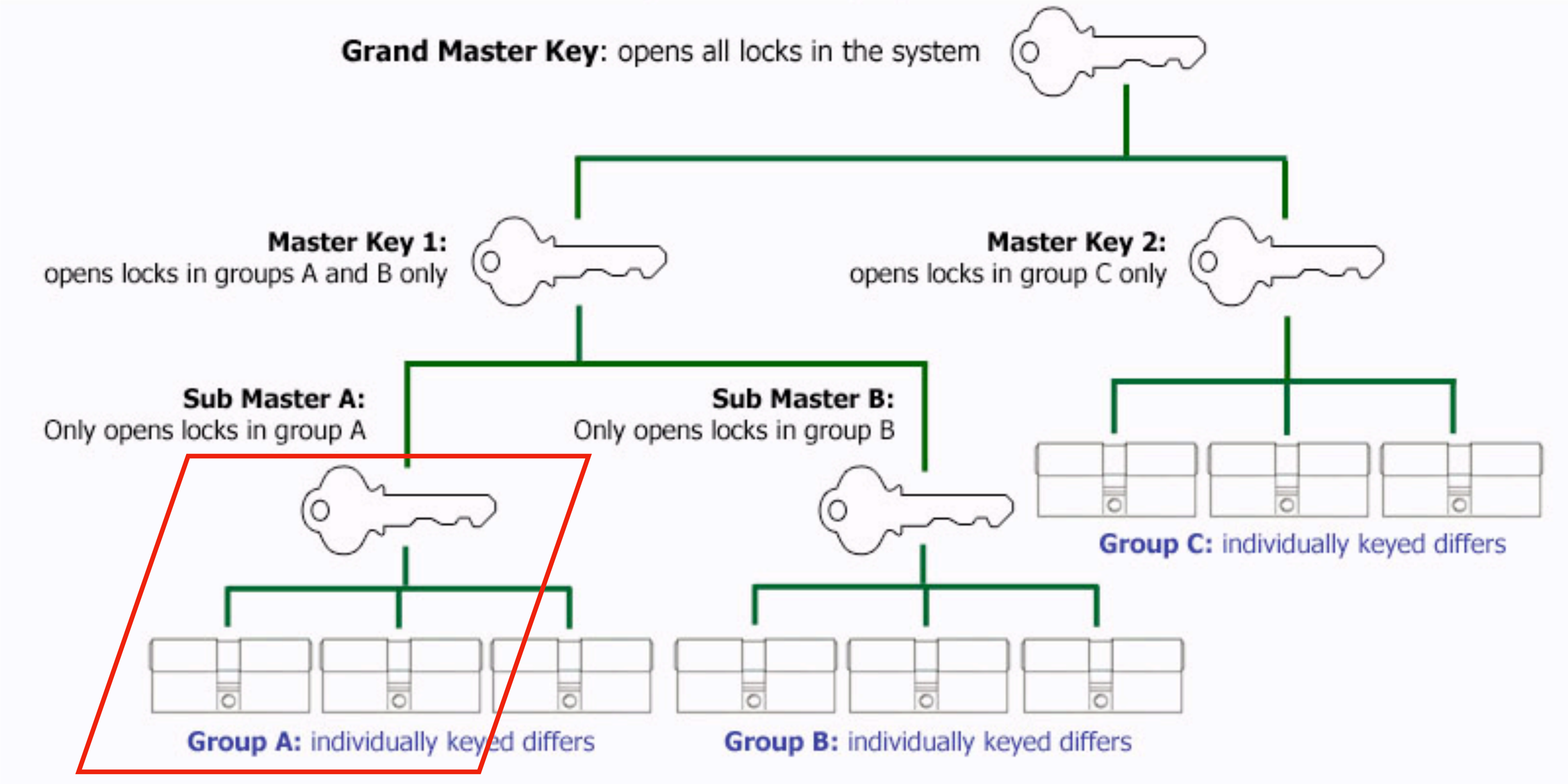


Bumping

https://www.youtube.com/watch?v=mmHPhI9X5B0

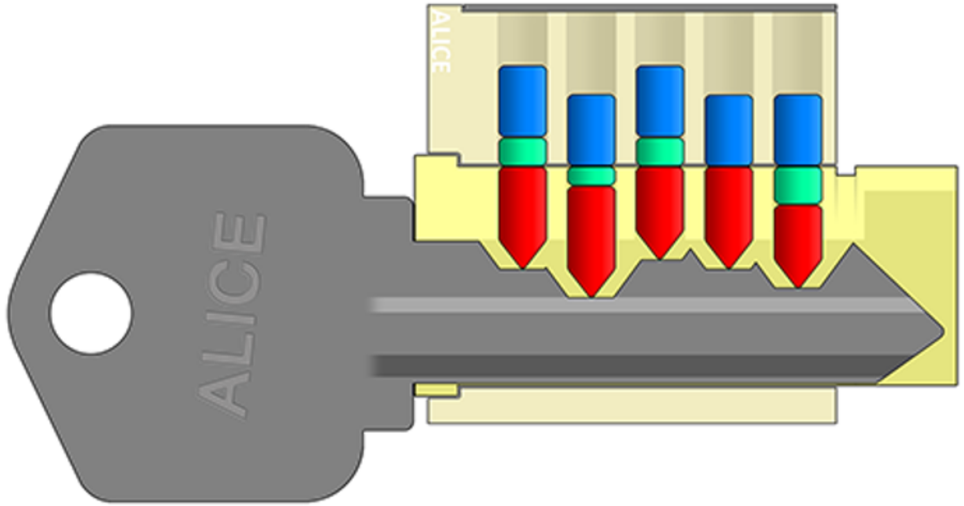
Master keying

MASTER KEY SYSTEM

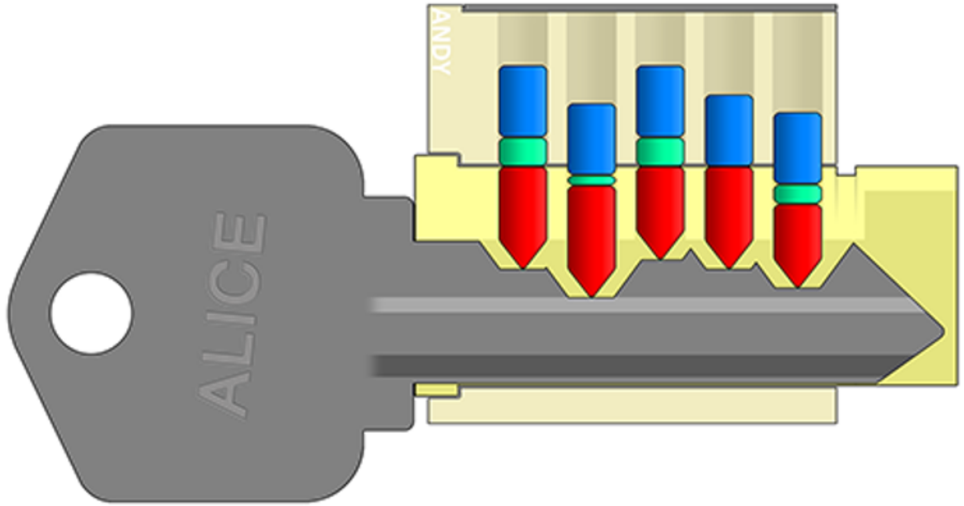


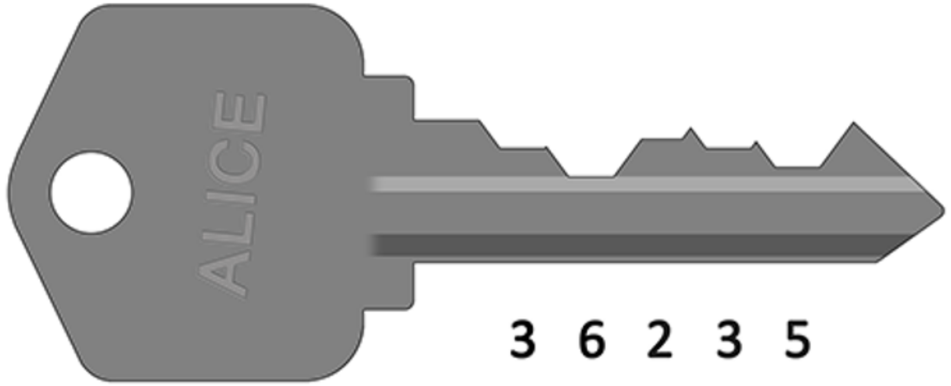
Source: https://www.arcolock.com/locksmith-office-master-keying/

ALICE



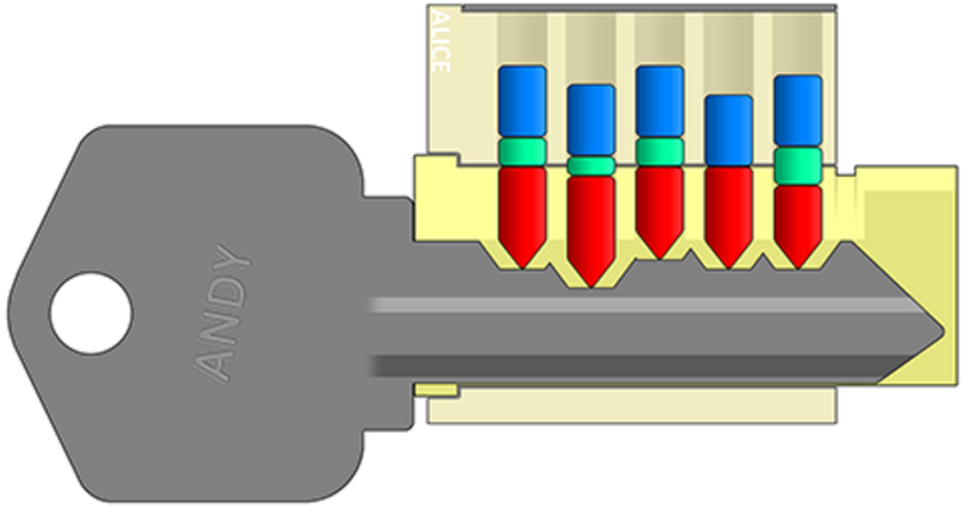
ANDY



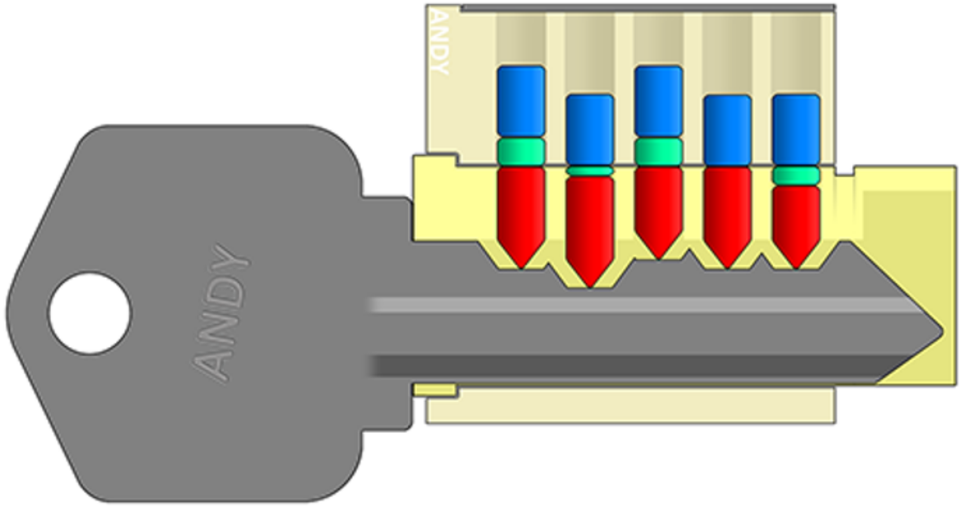


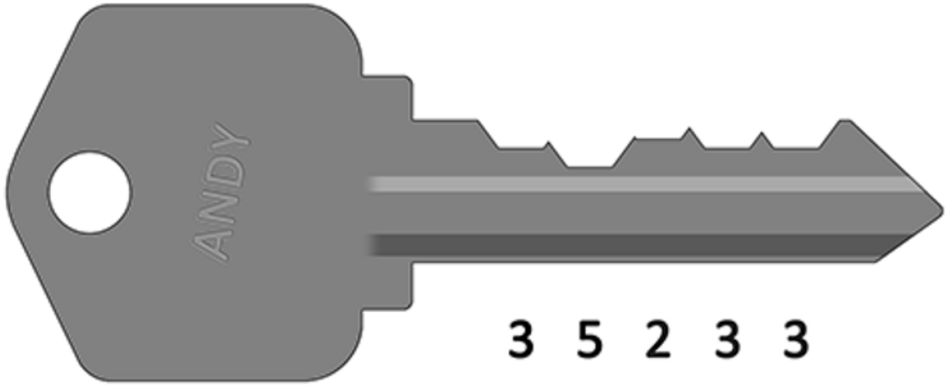
Source: https://deviating.net/lockpicking/slides.html

ALICE

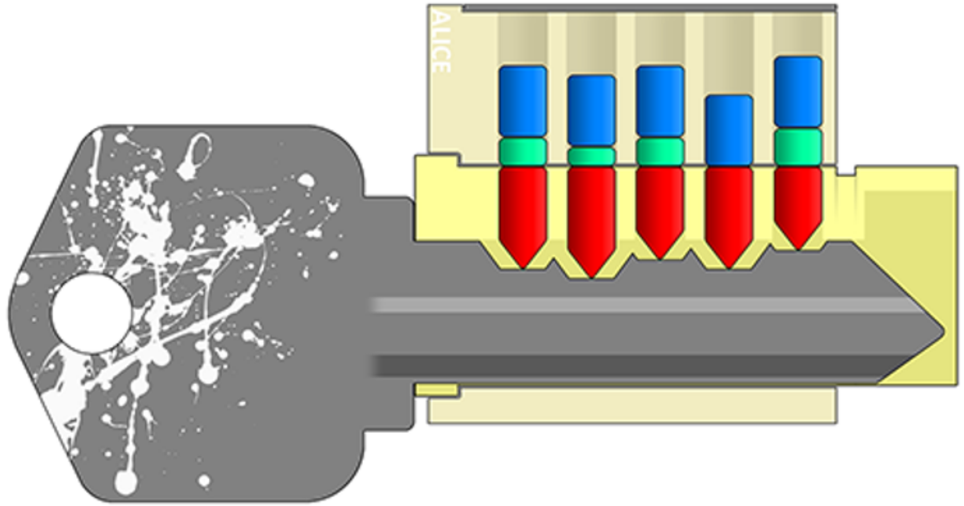


ANDY

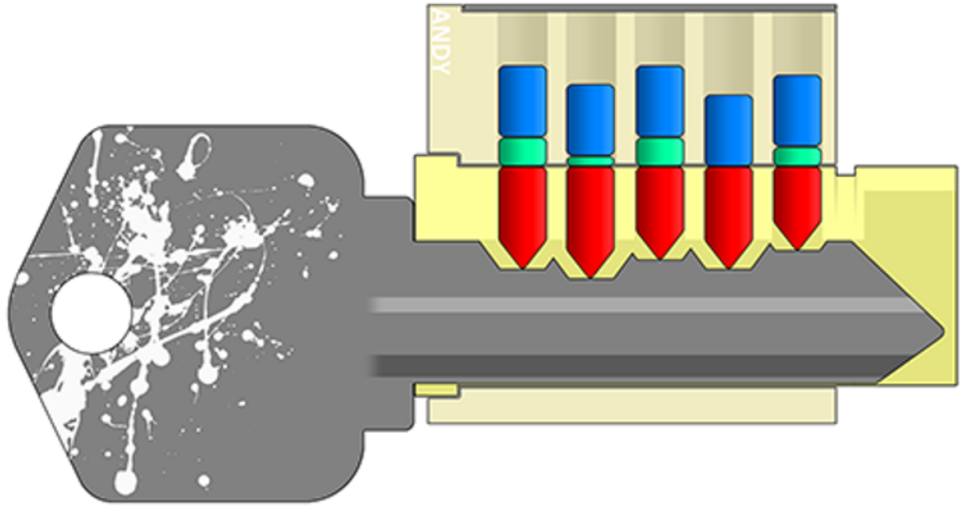


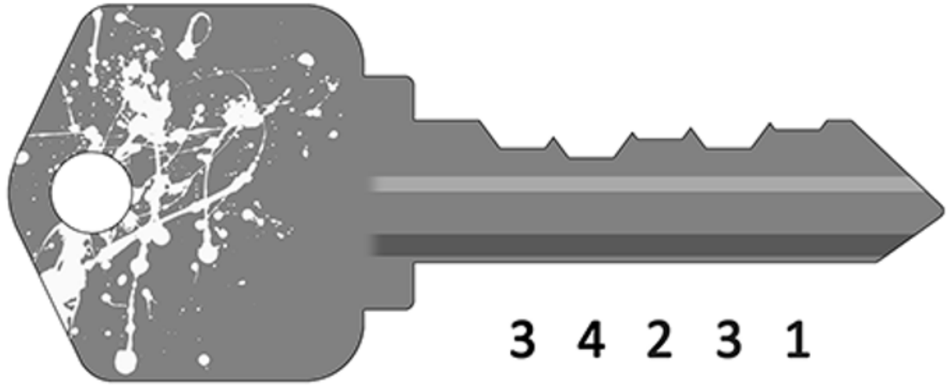


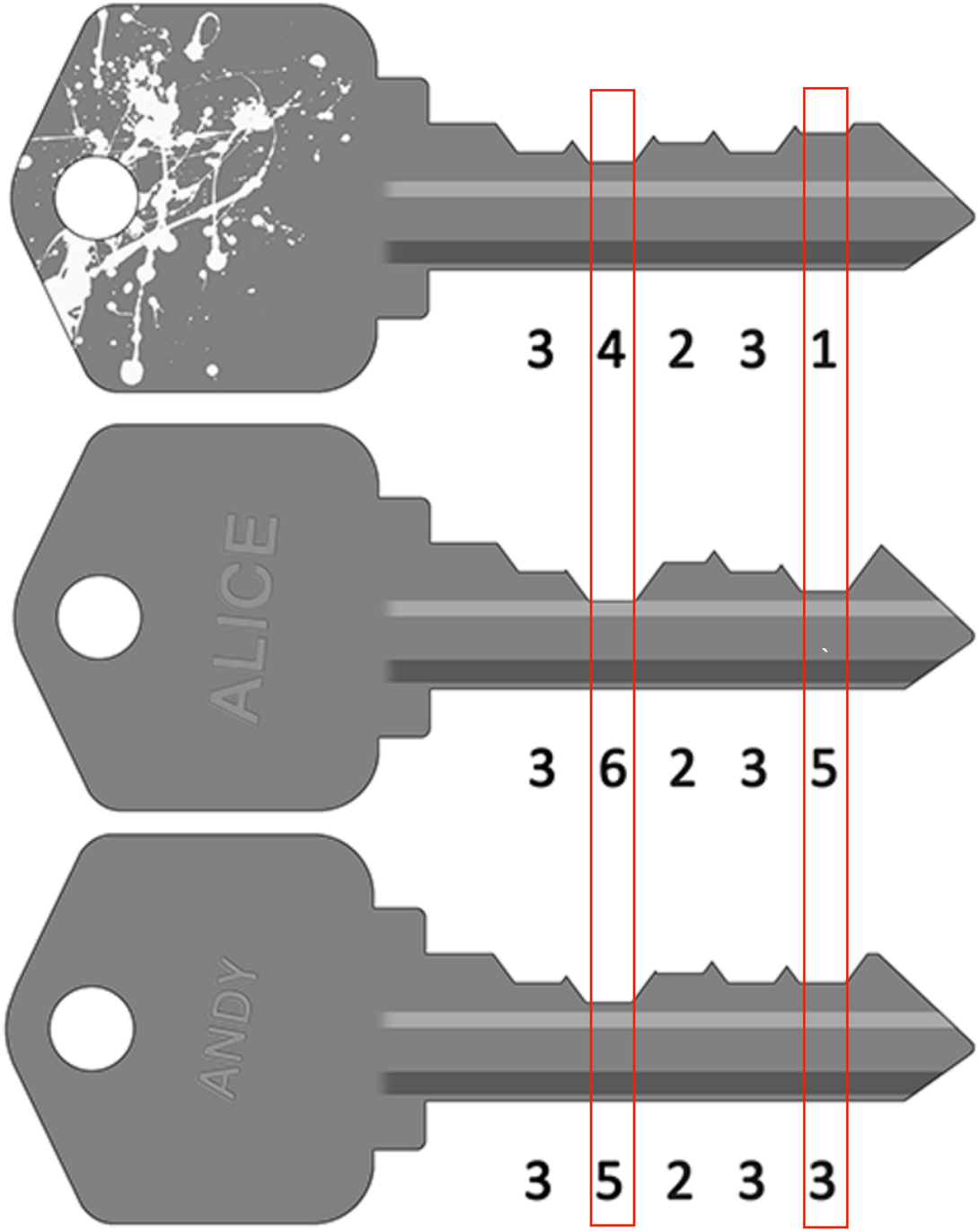
ALICE

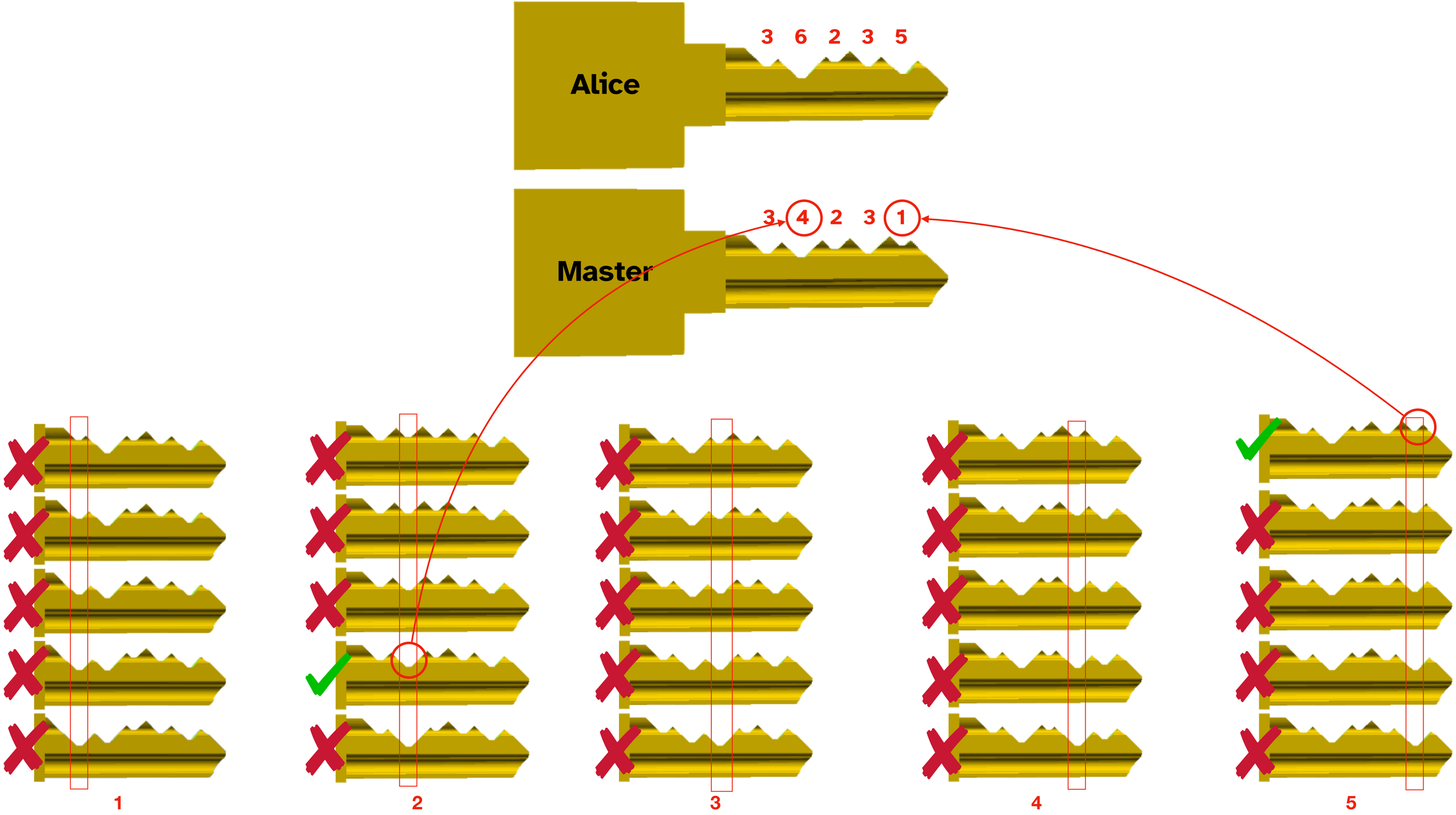


ANDY

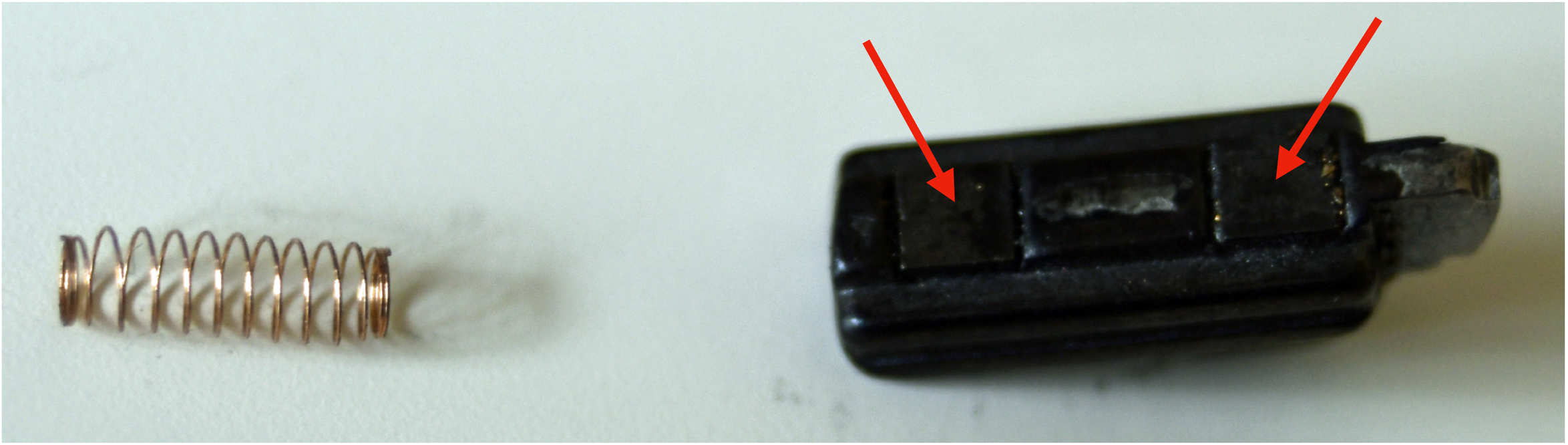


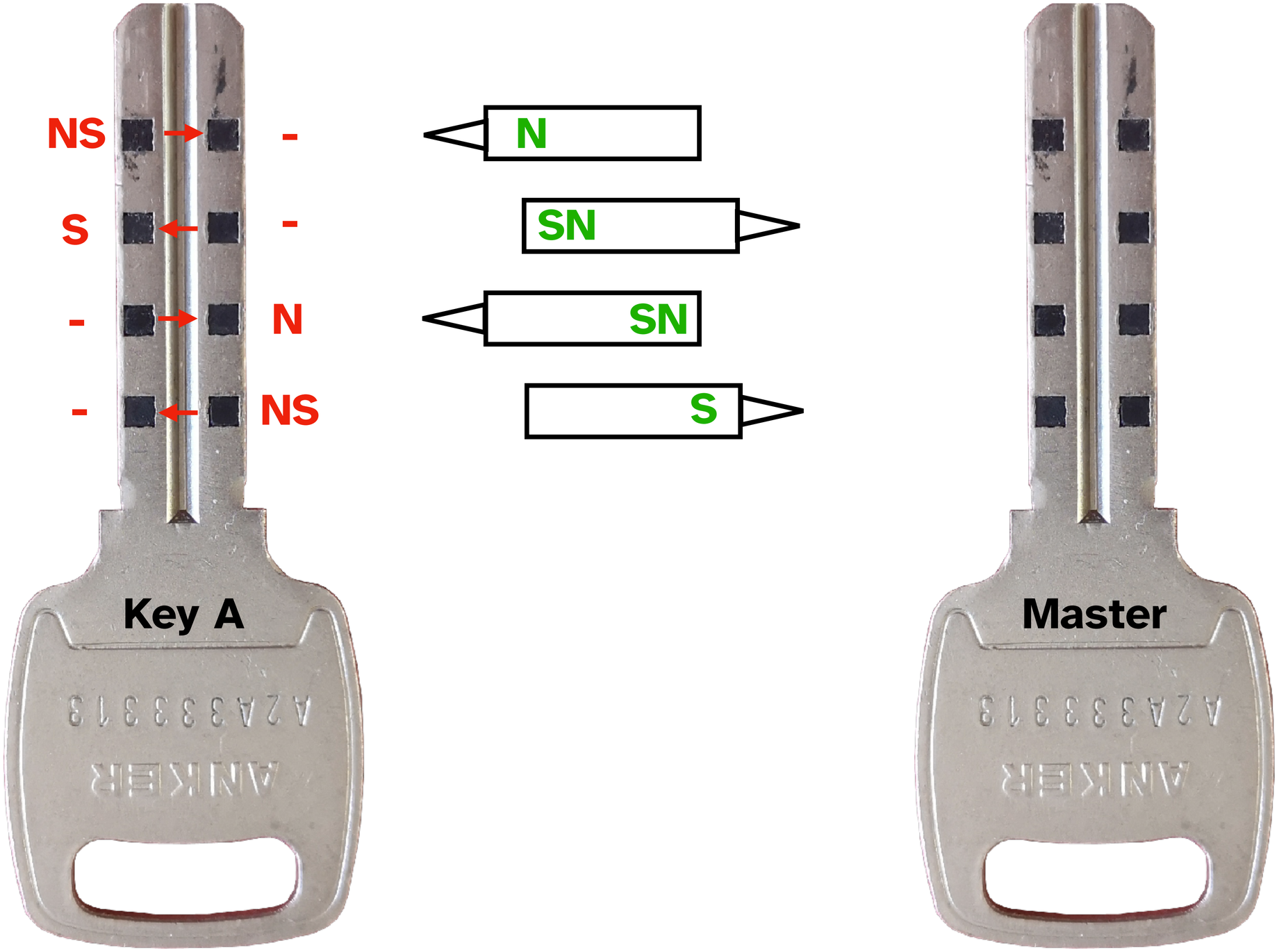


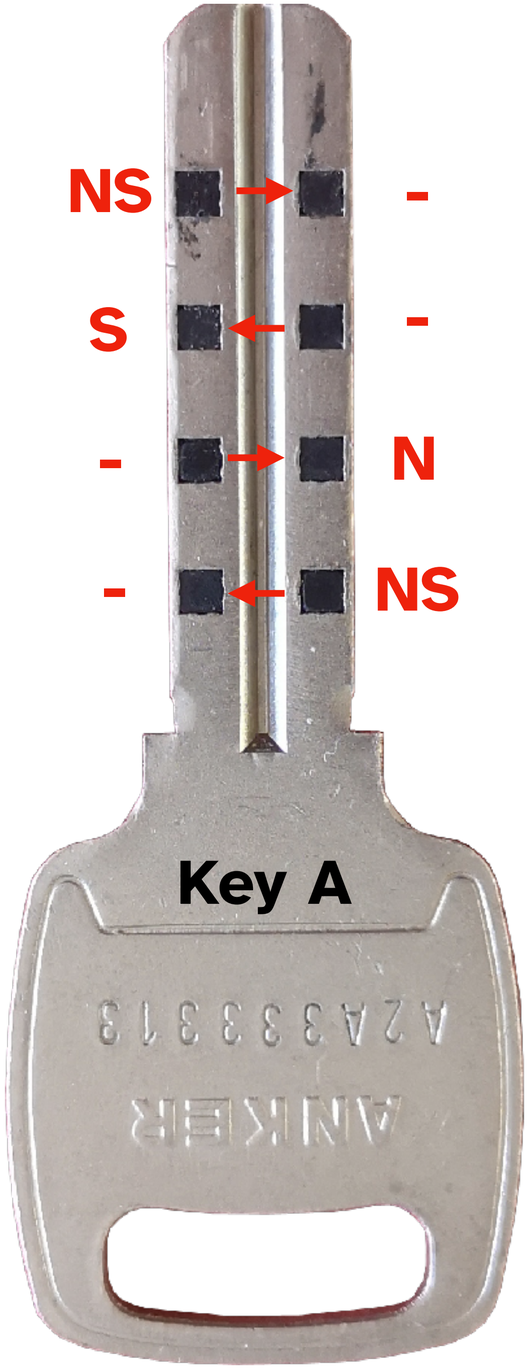

3 4 2 3 1
ALICE
3 6 2 3 5
ANDY
3 5 2 3 3

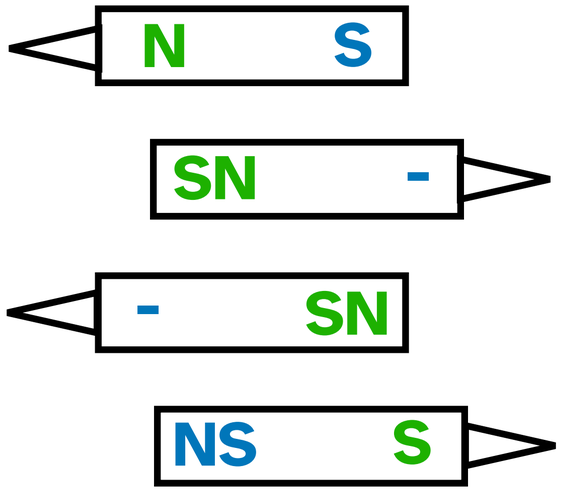

Alice
3 6 2 3 5
Master
3 4 2 3 1
1
2
3
4
5

Magnet master keying

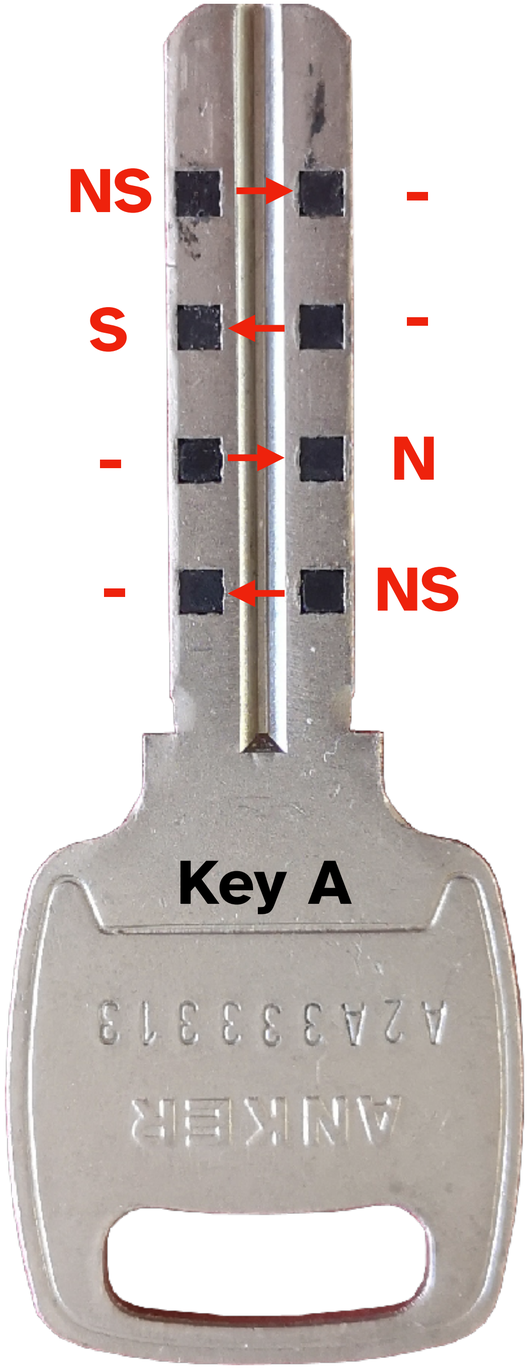


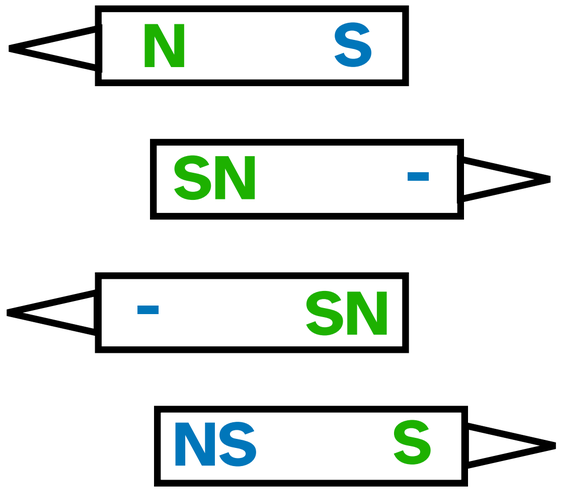

NS
S
-
-
-
-
NS
N
SN
SN
S
Key A
Master

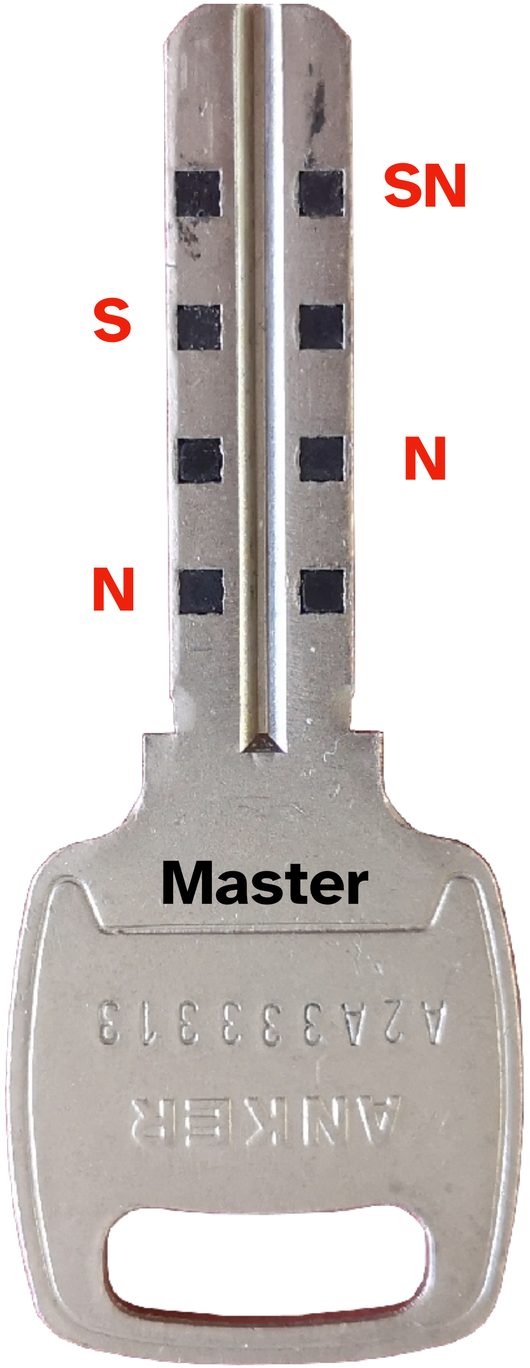




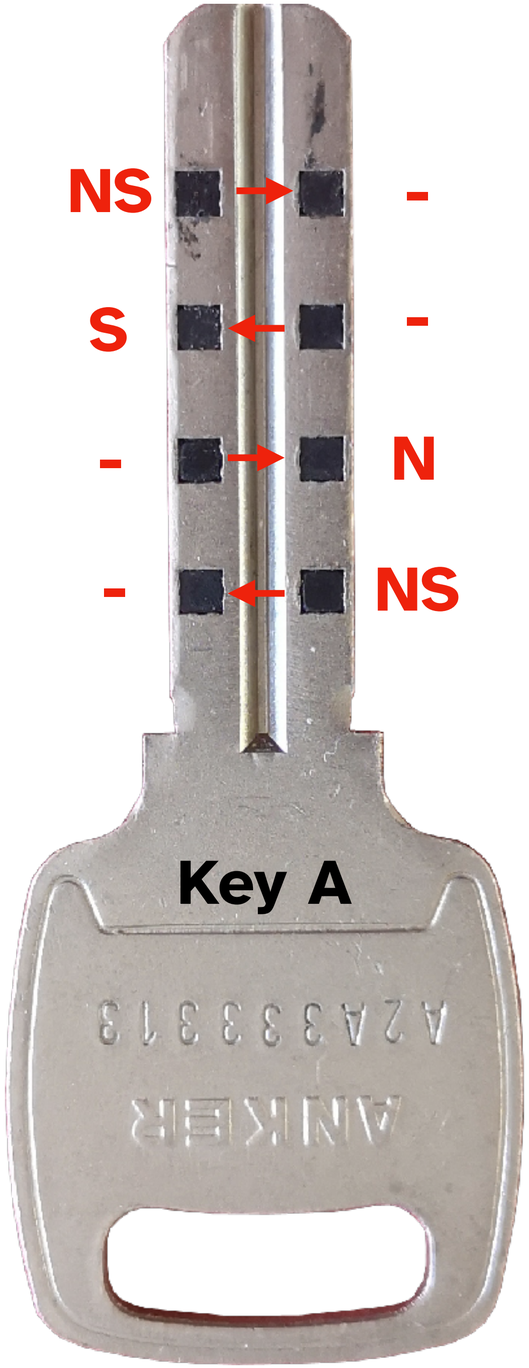
The master key will HAVE to have magnets to operate each slider

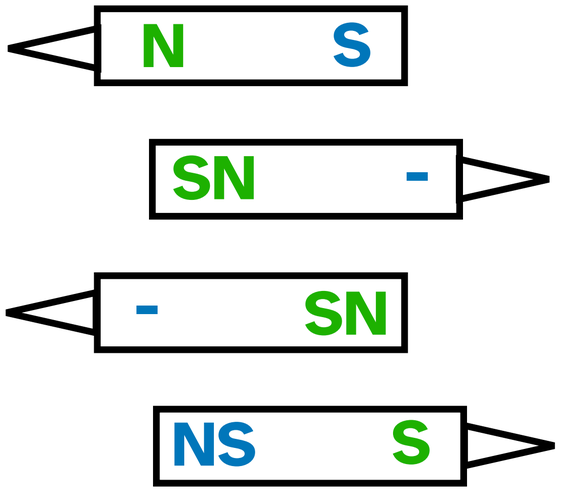


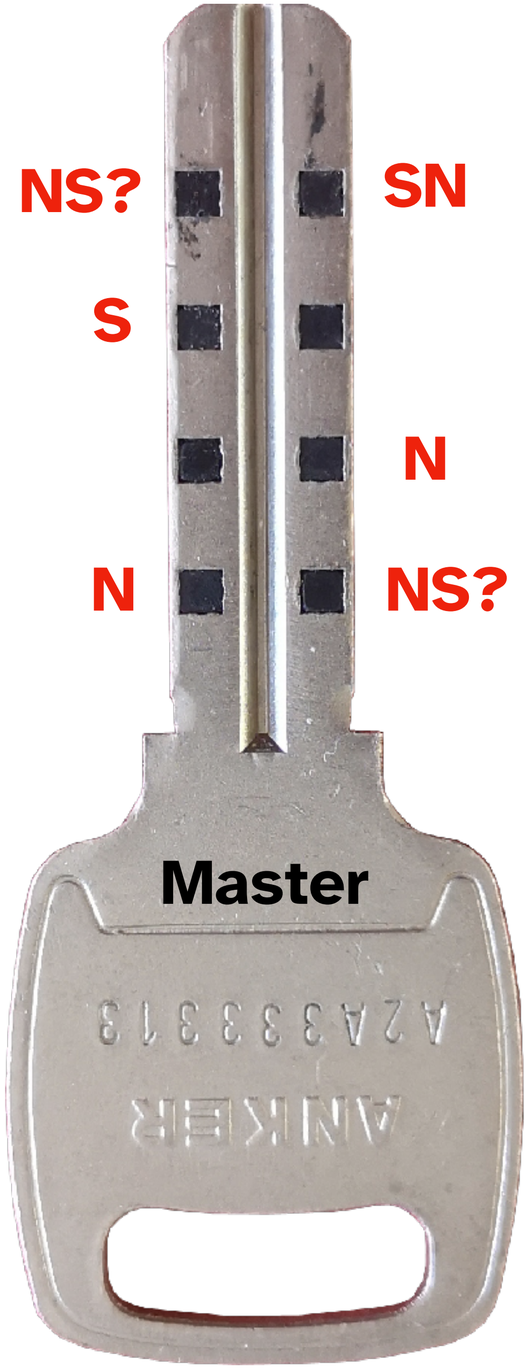




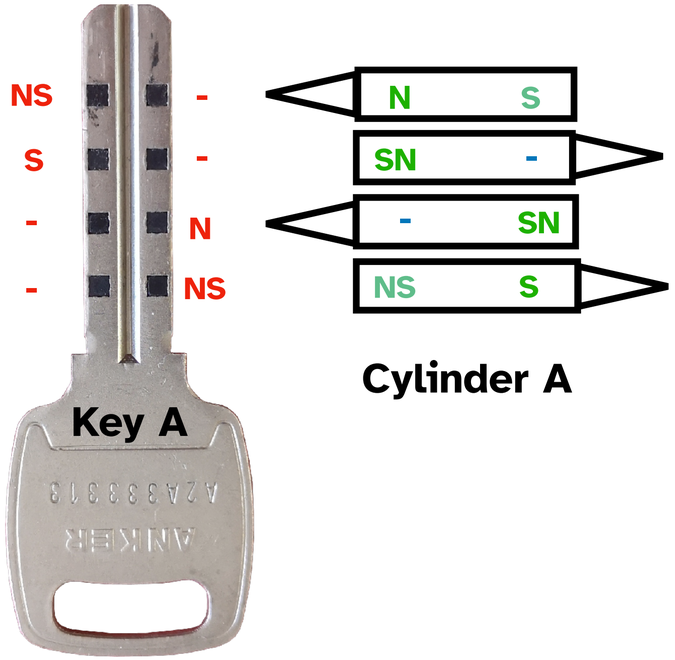
The master key will HAVE to have magnets that operate the 'blue' magnets in the cylinder

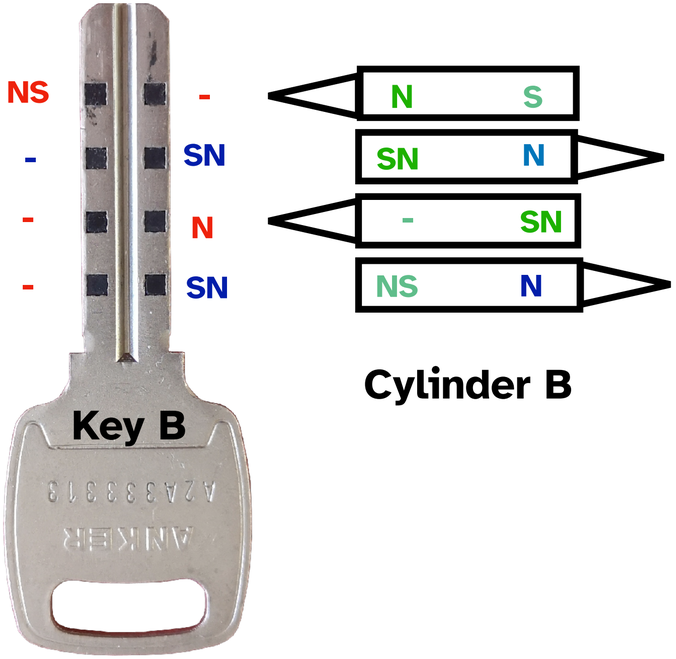




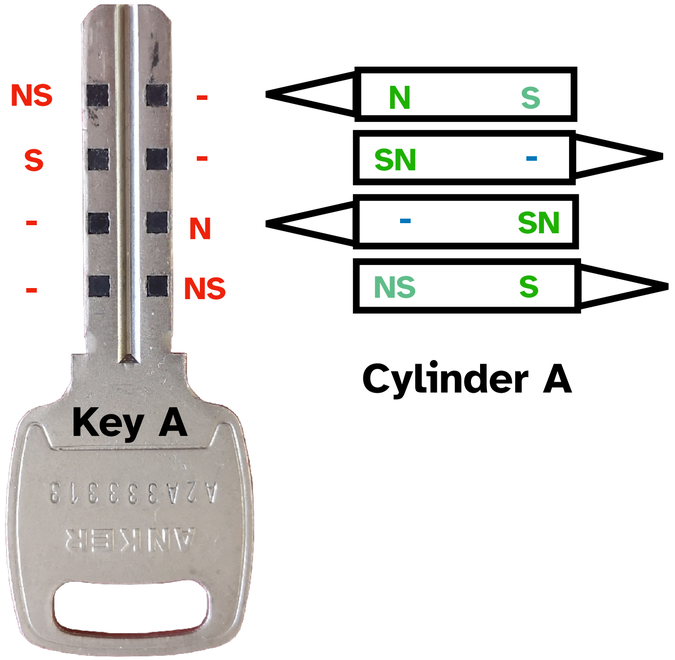


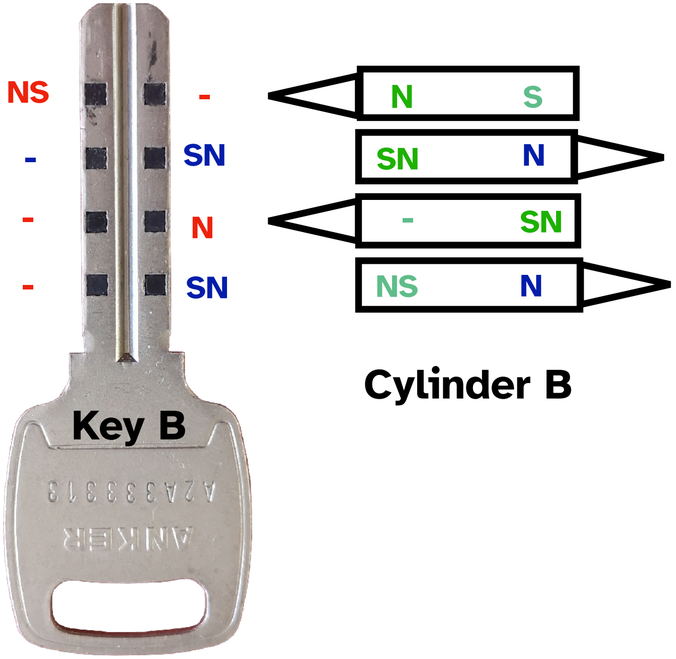
What to do with sliders with two magnets?

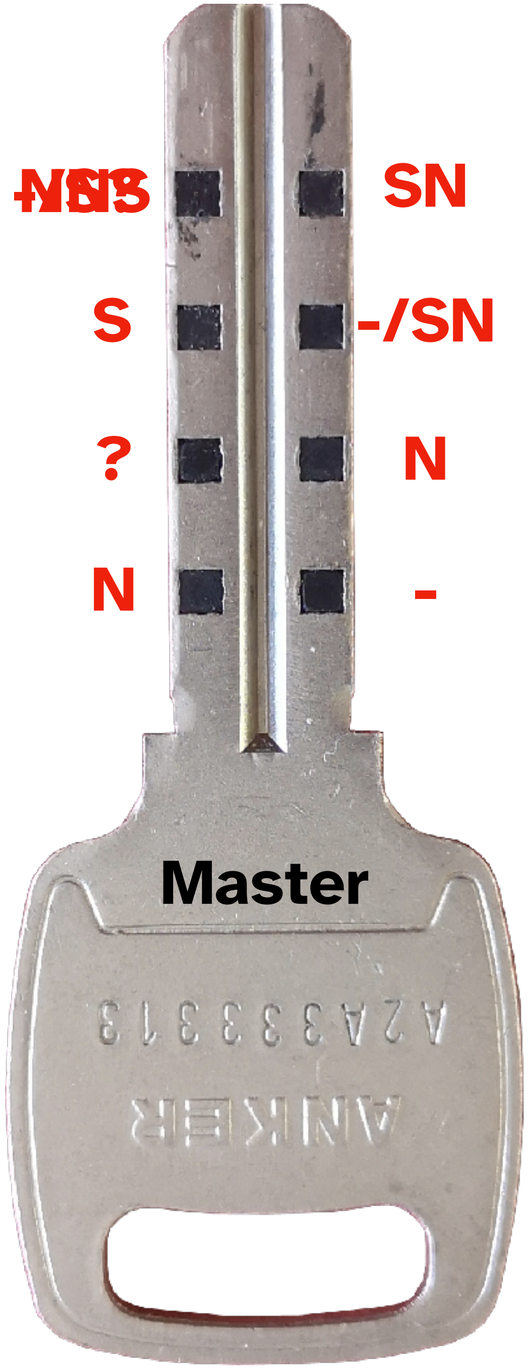

NS
S
-
-
-
-
N
NS
N S
SN -
- SN
NS S
Key A
Cylinder A

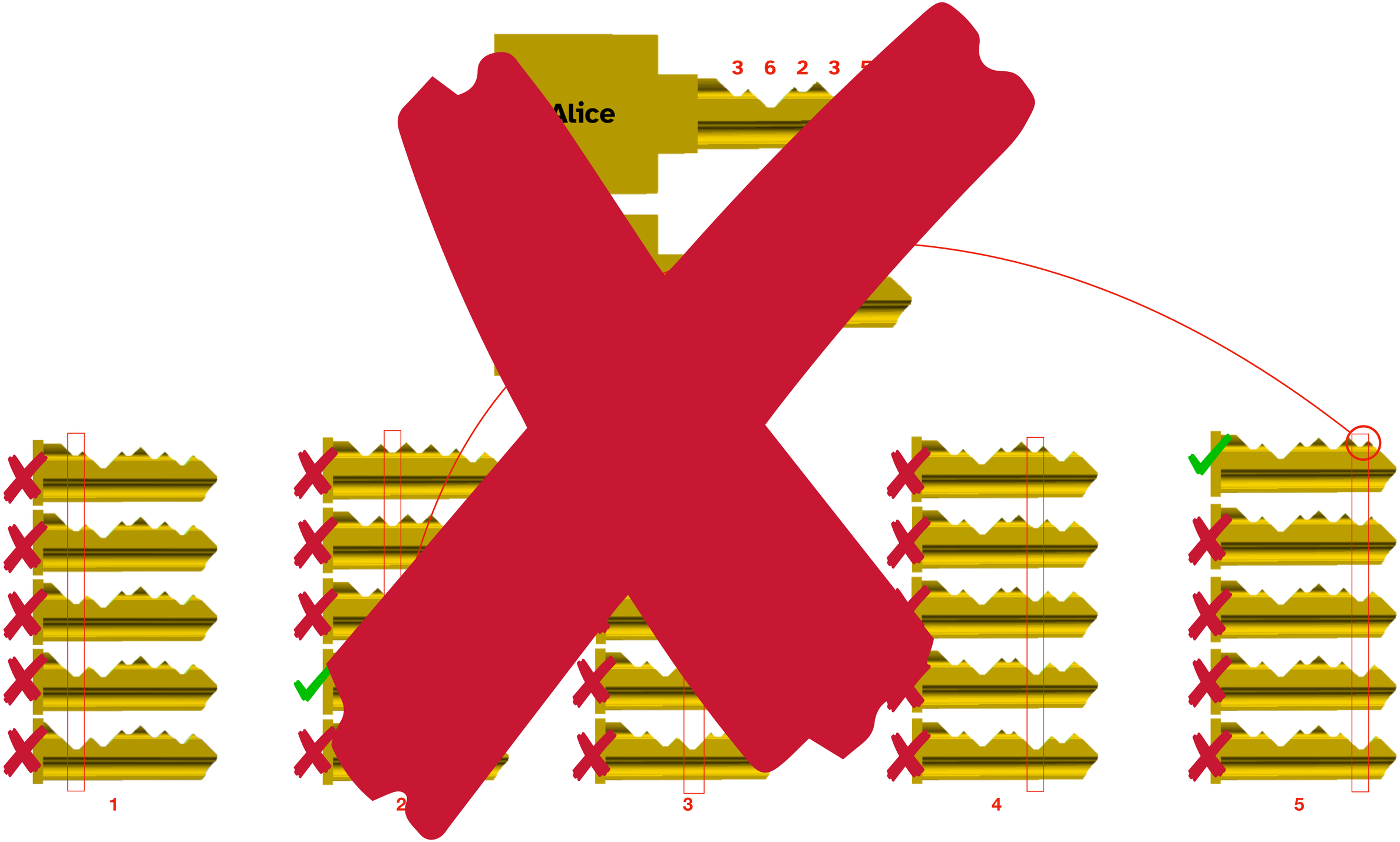

NS
-
-
-
SN
N
SN
N S
SN N
- SN
NS N
Key B
Cylinder B

NS?
S
N
NS?
SN
N
Master


NS
S
-
-
-
-
N
NS
N S
SN -
- SN
NS S
Key A
Cylinder A


NS
-
-
SN
-
N
-
SN
N S
SN N
- SN
NS N
Key B
Cylinder B

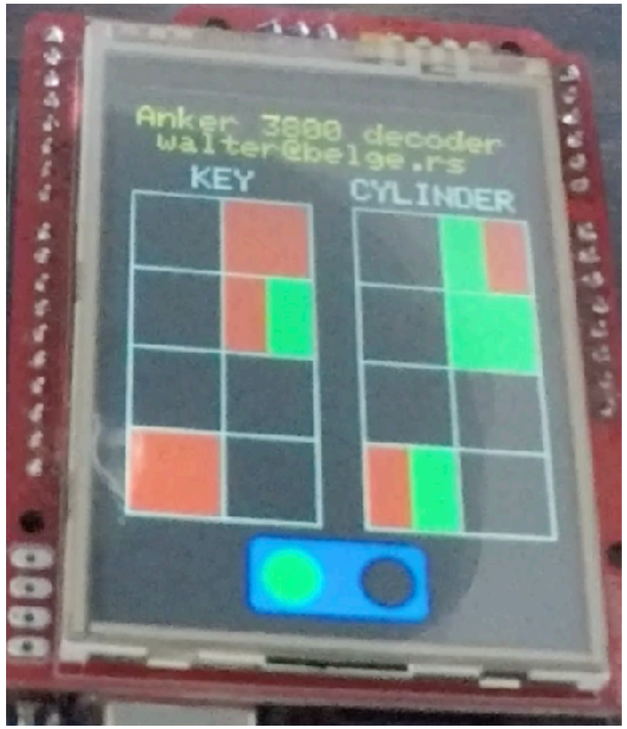

NS
SN
S
-/SN
?
N
N
-
Master


Alice
3 6 2 3
1
2
3
4
5

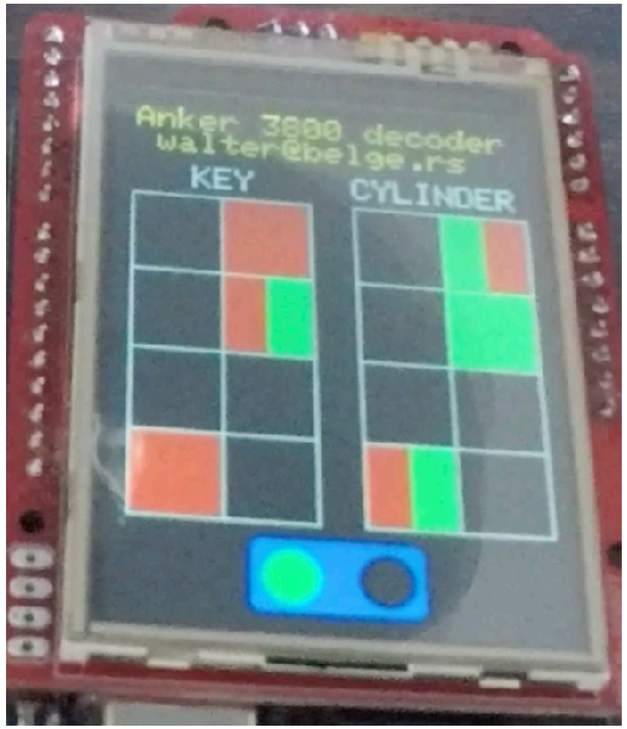
Use case

#	Cyl		Key		MK
1					
2					
3					
4					
5 (half)					

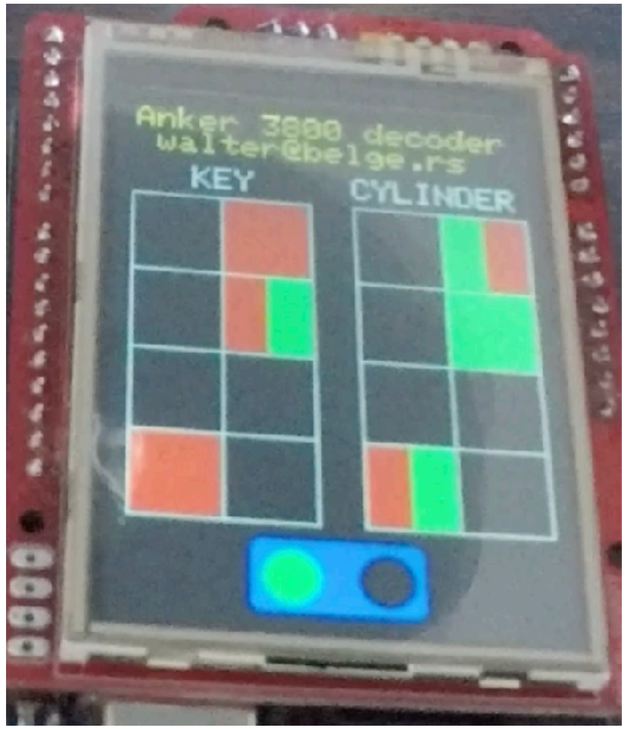
#	Cyl			Key		MK
1	RG - GR GR	R G - GR				
2	GR - GR RG	R G - GR				
3	R - GR RG	R G - GR				
4	GR - GR -	R G - GR				
5 (half)	GR - GR -	R G - GR				



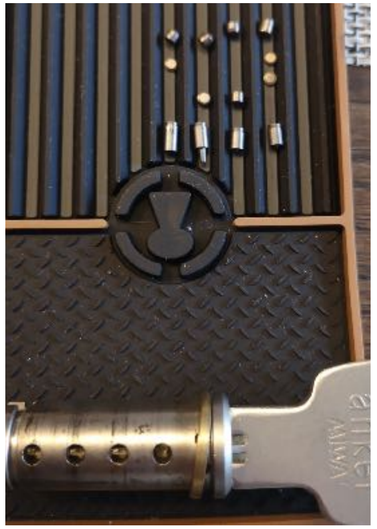
#	Cyl			Key		MK	
1	RG - GR GR	R G - GR				- - R -	RG RG - G
2	GR - GR RG	R G - GR					
3	R - GR RG	R G - GR					
4	GR - GR -	R G - GR					
5 (half)	GR - GR -	R G - GR					

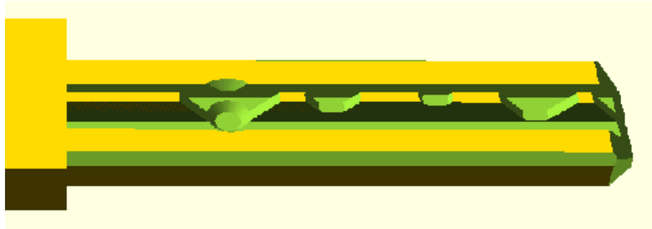


#	Cyl			Key			MK	
1	RG	R		G	-		-	RG
	-	G		-	RG		-	RG
	GR	-		R	-		R	-
	GR	GR		G	-		-	G
2	GR	R		R	-			
	-	G		-	RG			
	GR	-		R	-			
	RG	GR		R	-			
3	R	R		RG	-			
	-	G		-	RG			
	GR	-		R	-			
	RG	GR		R	-			
4	GR	R		R	-			
	-	G		-	RG			
	GR	-		R	-			
	-	GR		-	G			
5 (half)	GR	R		R	-			
	-	G		-	RG			
	GR	-		R	-			
	-	GR		-	G			

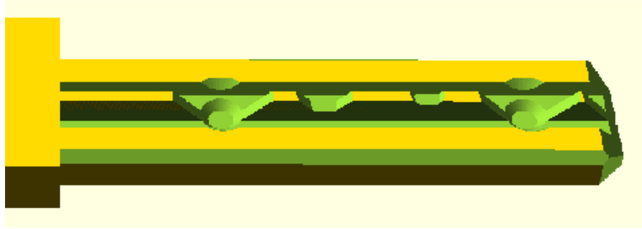


#	Cyl				Key			MK	
1	RG - GR GR		R G - GR		G - R G	- RG - -		- - R -	RG RG - G
2	GR - GR RG		R G - GR		R - R R	- RG - -			
3	R - GR RG		R G - GR		RG - R R	- RG - -			
4	GR - GR -		R G - GR		R - R -	- RG - G			
5 (half)	GR - GR -	3/4 1/3 2/3 4	R G - GR		R - R -	- RG - G			

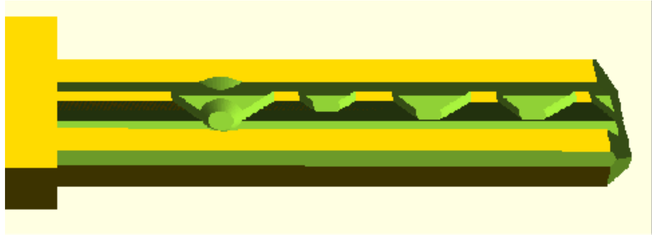




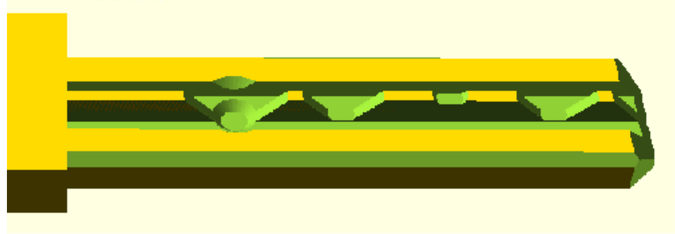
4213



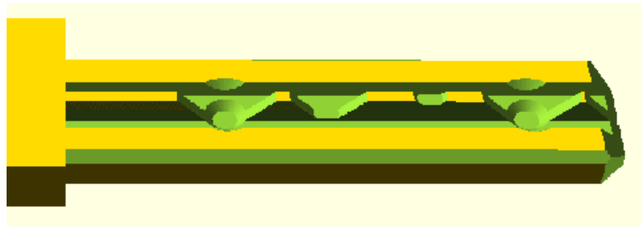
4214



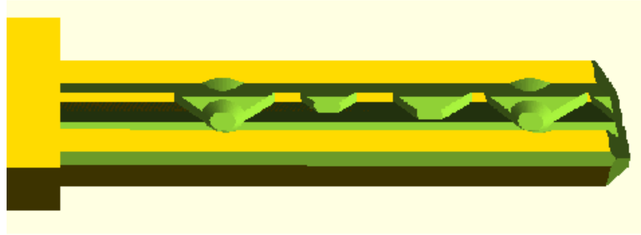
4133



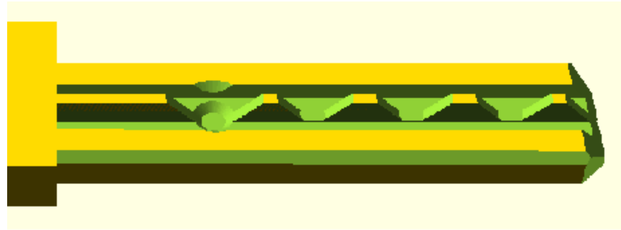
4313



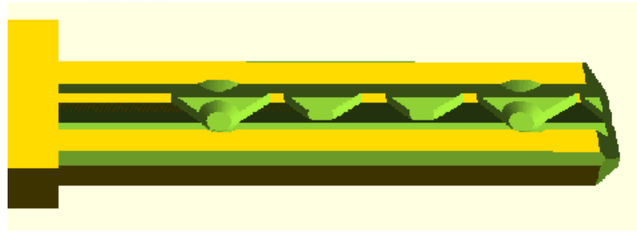
4314



4234

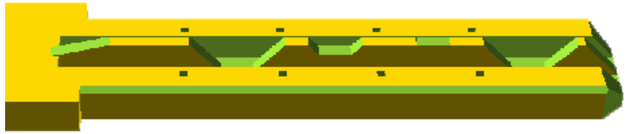


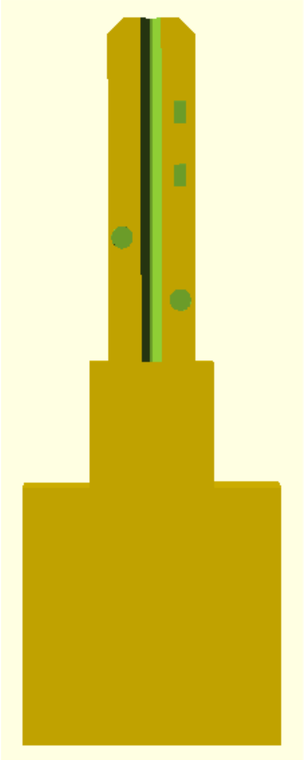
4333

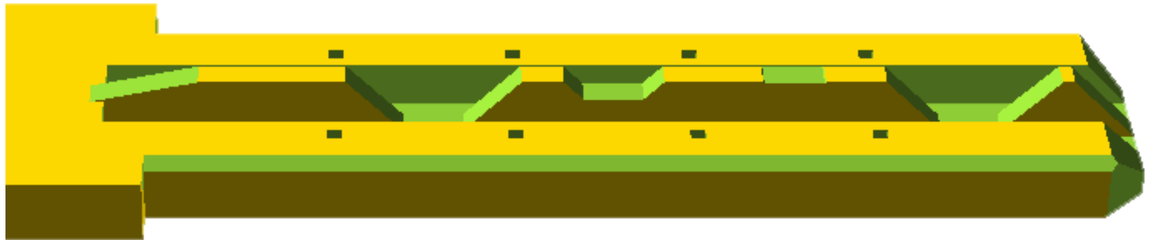


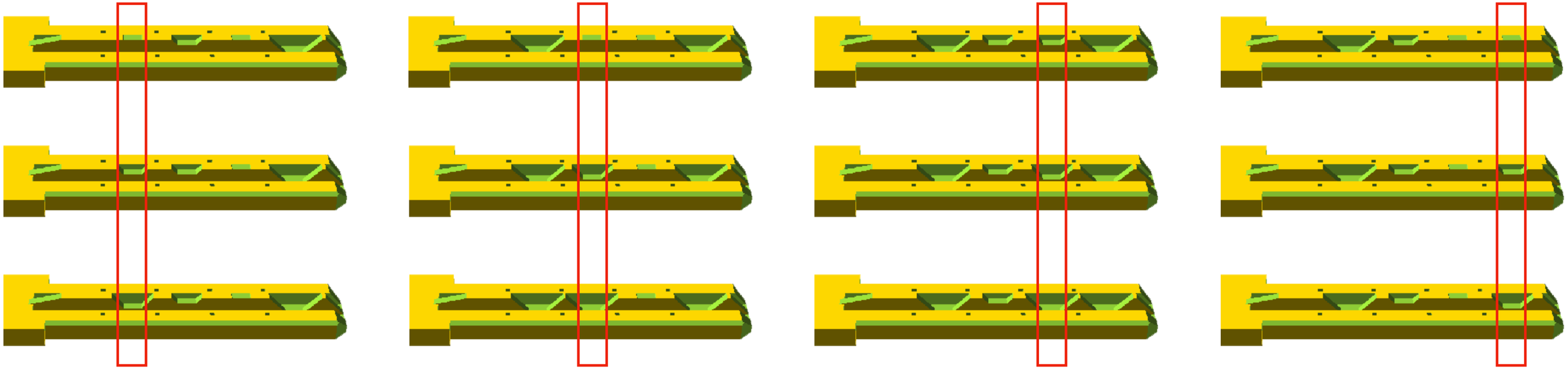
4334

#	Cyl				Key			MK		
1	RG - GR GR		R G - GR		G - R G	- RG - -		- ? R -	4 1 2 4	RG RG ? G
2	GR - GR RG		R G - GR		R - R R	- RG - -				
3	R - GR RG		R G - GR		RG - R R	- RG - -				
4	GR - GR -		R G - GR		R - R -	- RG - G				
5 (half)	GR - GR -	3/4 1/3 2/3 4	R G - GR		R - R -	- RG - G				







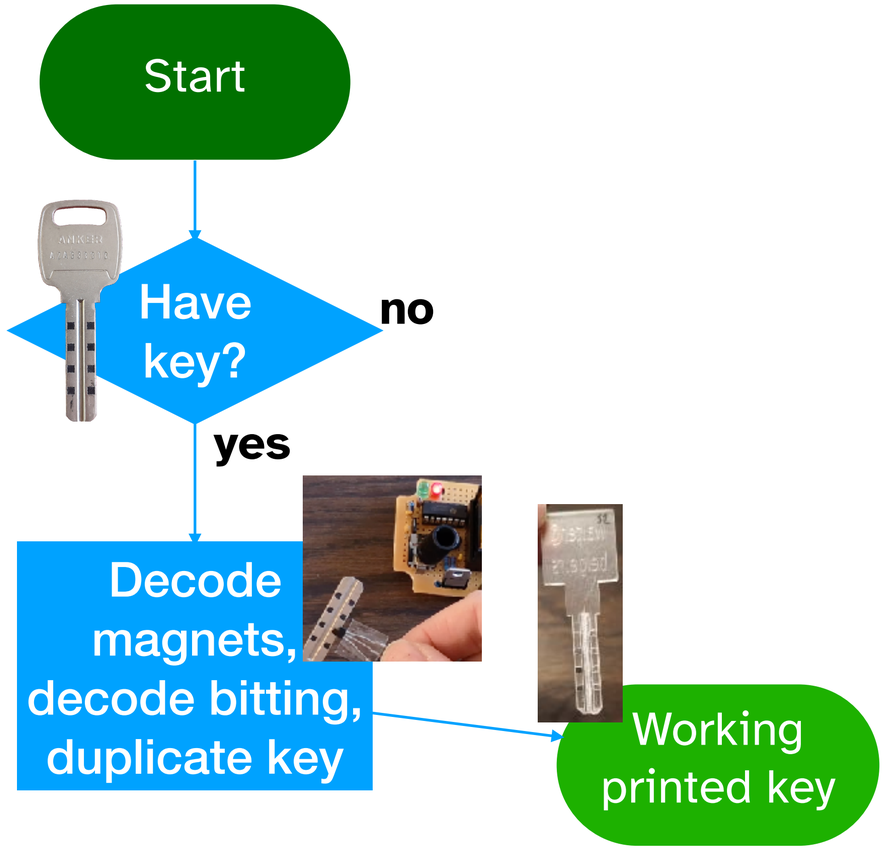


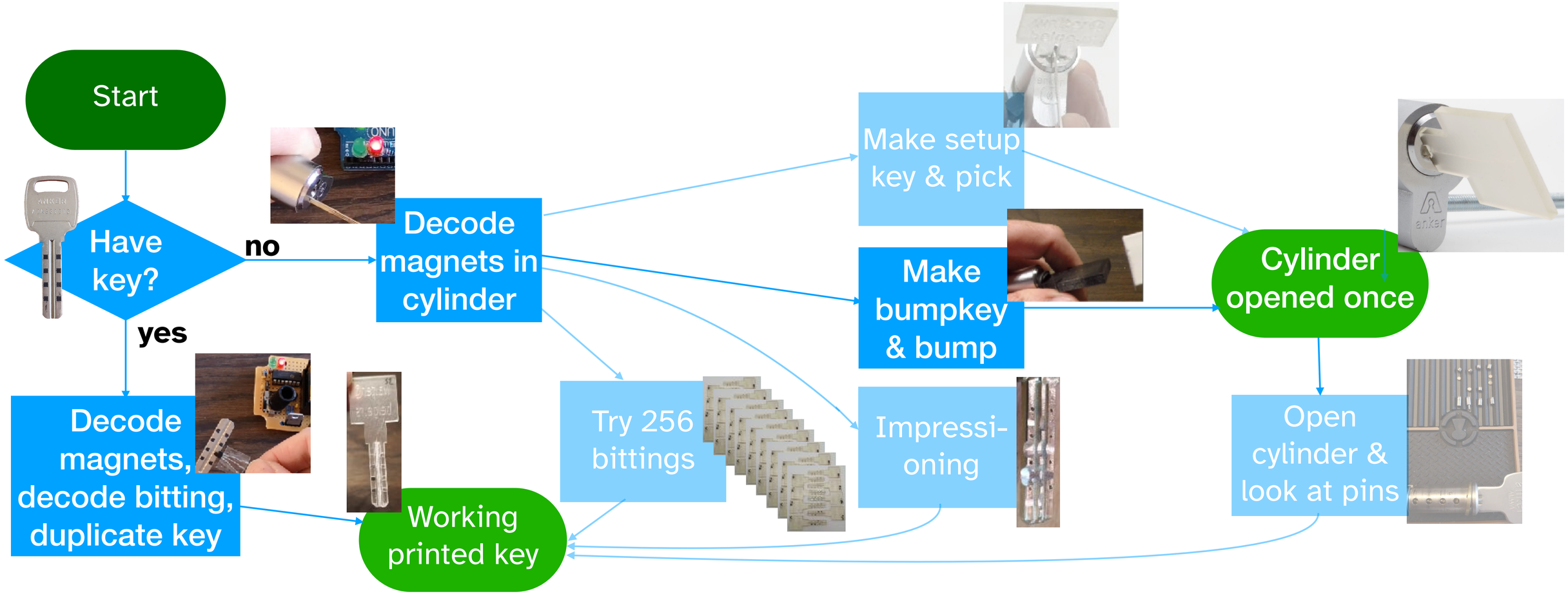
#	Cyl				Key			MK		
1	RG	3/4	R		G	-		-	4	RG
	-	1/2	G		-	RG		-	1	RG
	GR	2/3	-		R	-		R	2	-
	GR	4	GR		G	-		-	4	G
2	GR	3/4	R		R	-				
	-	1	G		-	RG				
	GR	2/3	-		R	-				
	RG	4	GR		R	-				
3	R	3/4	R		RG	-				
	-	1/4	G		-	RG				
	GR	2	-		R	-				
	RG	3/4	GR		R	-				
4	GR	1/4	R		R	-				
	-	1/4	G		-	RG				
	GR	2/4	-		R	-				
	-	4	GR		-	G				
5 (half)	GR	3/4	R		R	-				
	-	1/3	G		-	RG				
	GR	2/3	-		R	-				
	-	4	GR		-	G				

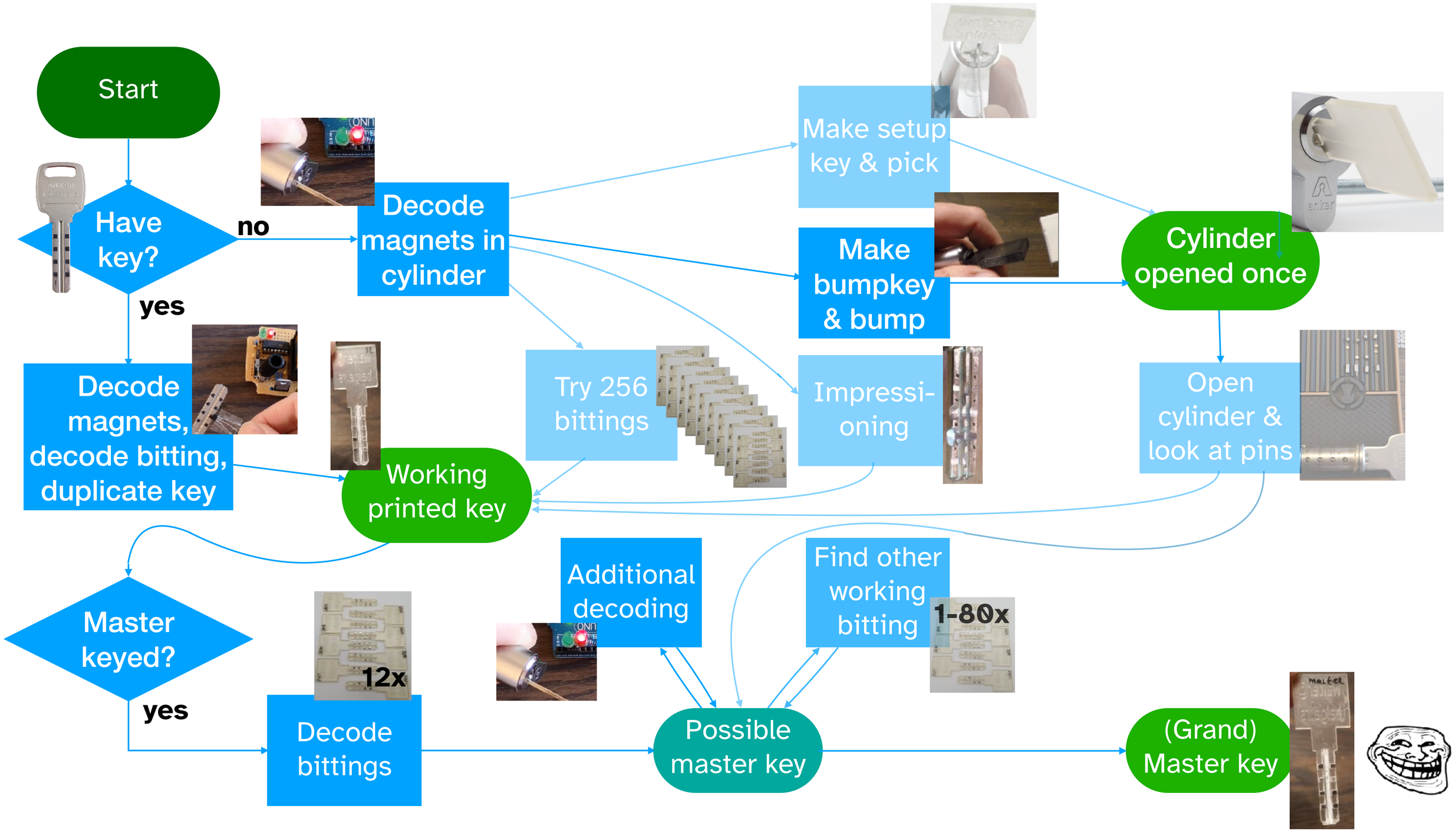
#	Cyl				Key				MK		
1	RG	3/4	R		G	3	-		-	4	RG
	-	1/2	G		-	2	RG		-	1	RG
	GR	2/3	-		R	3	-		R	2	-
	GR	4	GR		G	4	-		-	4	G
2	GR	3/4	R		R	3	-				
	-	1	G		-	1	RG				
	GR	2/3	-		R	3	-				
	RG	4	GR		R	4	-				
3	R	3/4	R		RG	3	-				
	-	1/4	G		-	4	RG				
	GR	2	-		R	2	-				
	RG	3/4	GR		R	3	-				
4	GR	1/4	R		R	1	-				
	-	1/4	G		-	4	RG				
	GR	2/4	-		R	4	-				
	-	4	GR		-	4	G				
5 (half)	GR	3/4	R		R	3	-				
	-	1/3	G		-	3	RG				
	GR	2/3	-		R	3	-				
	-	4	GR		-	4	G				

3

Summarising


Start
Have key?
no
yes
Decode magnets, decode bitting, duplicate key
Working printed key

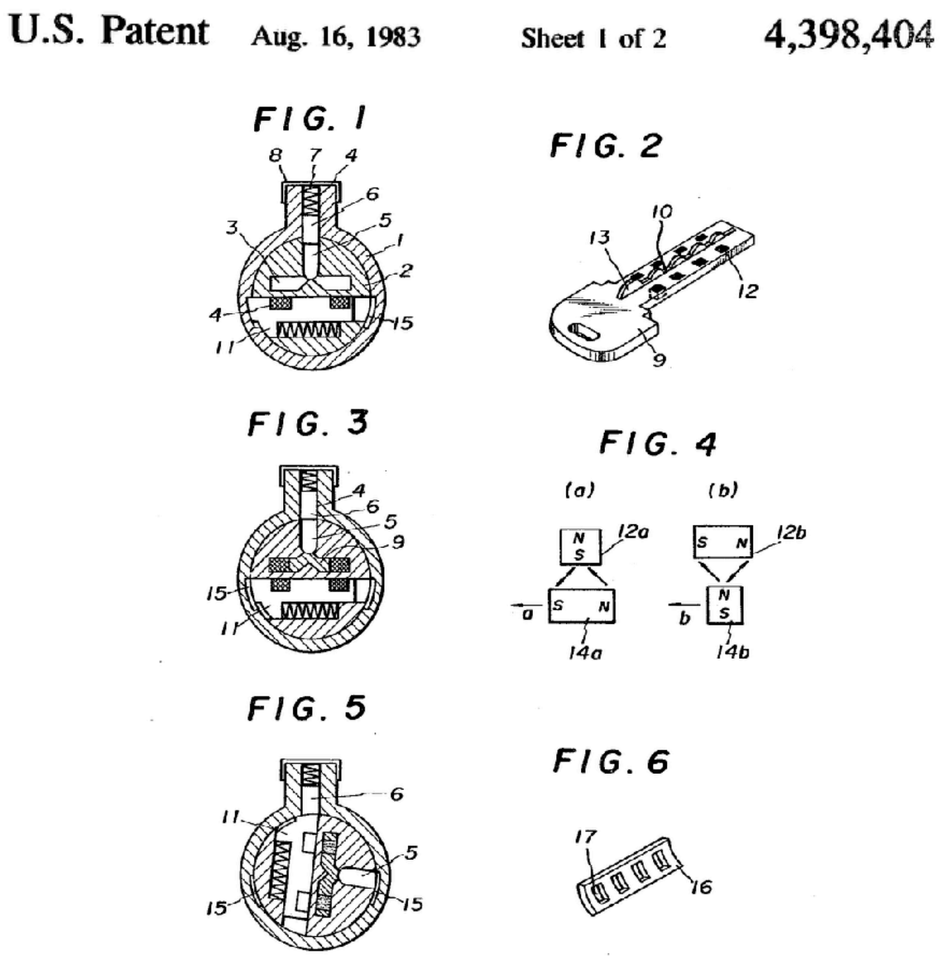

Start
Have key?
no
yes
Decode magnets in cylinder
Decode magnets, decode bitting, duplicate key
Working printed key
Make setup key & pick
Make bumpkey & bump
Try 256 bittings
Impressi-oning
Cylinder opened once
Open cylinder & look at pins


Start
Have key?
no
yes
Decode magnets in cylinder
Make setup key & pick
Make bumpkey & bump
Cylinder opened once
Decode magnets, decode bitting, duplicate key
Working printed key
Try 256 bittings
Impressi-oning
Open cylinder & look at pins
Master keyed?
yes
12x
Decode bittings
Additional decoding
Find other working bitting
1-80x
Possible master key
(Grand) Master key

Conclusion

- With the advent of 3D printers, almost all vendors have to deal with key copying attacks that were not possible earlier

- To duplicate this key it also required to decode the magnets from the cylinder



Conclusion

- Finding the (grand) master key still requires quite some work, more than with conventional locks

- And please: do not test stuff on cylinders that are not yours and/or that are in use

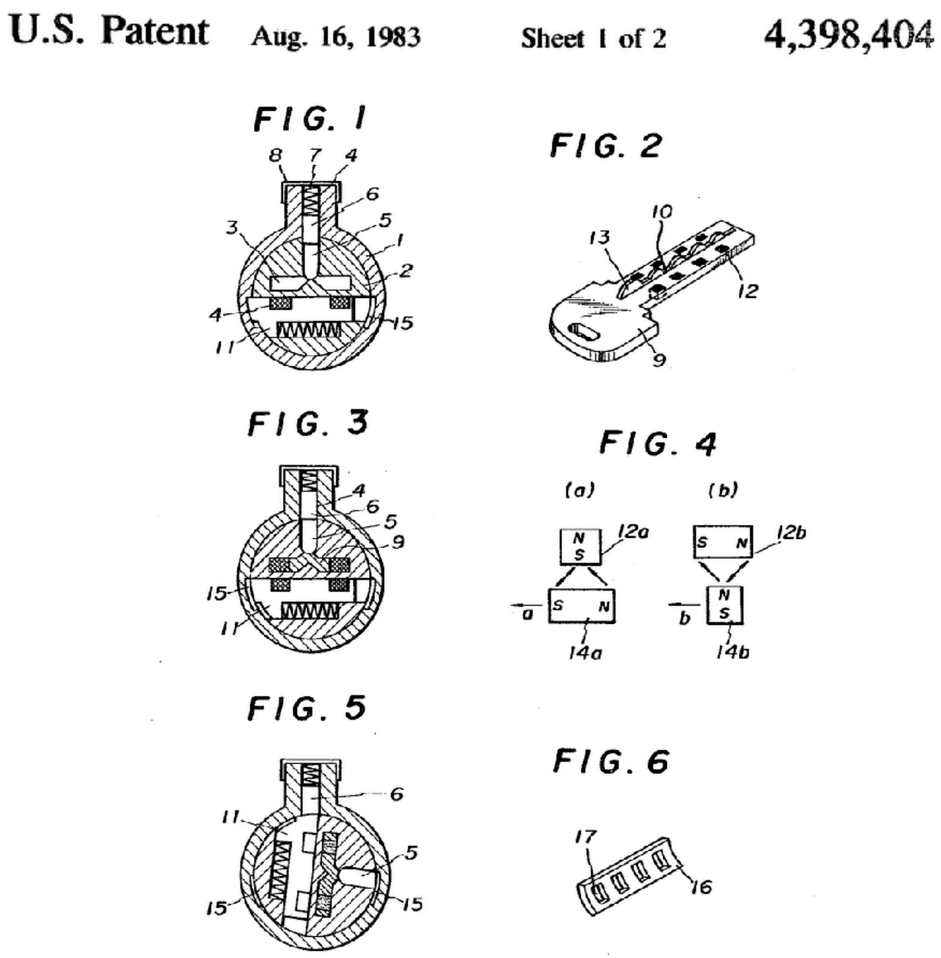


Image: Working Title Films