What if locks could talk; what stories would they tell?

Jan-Willem

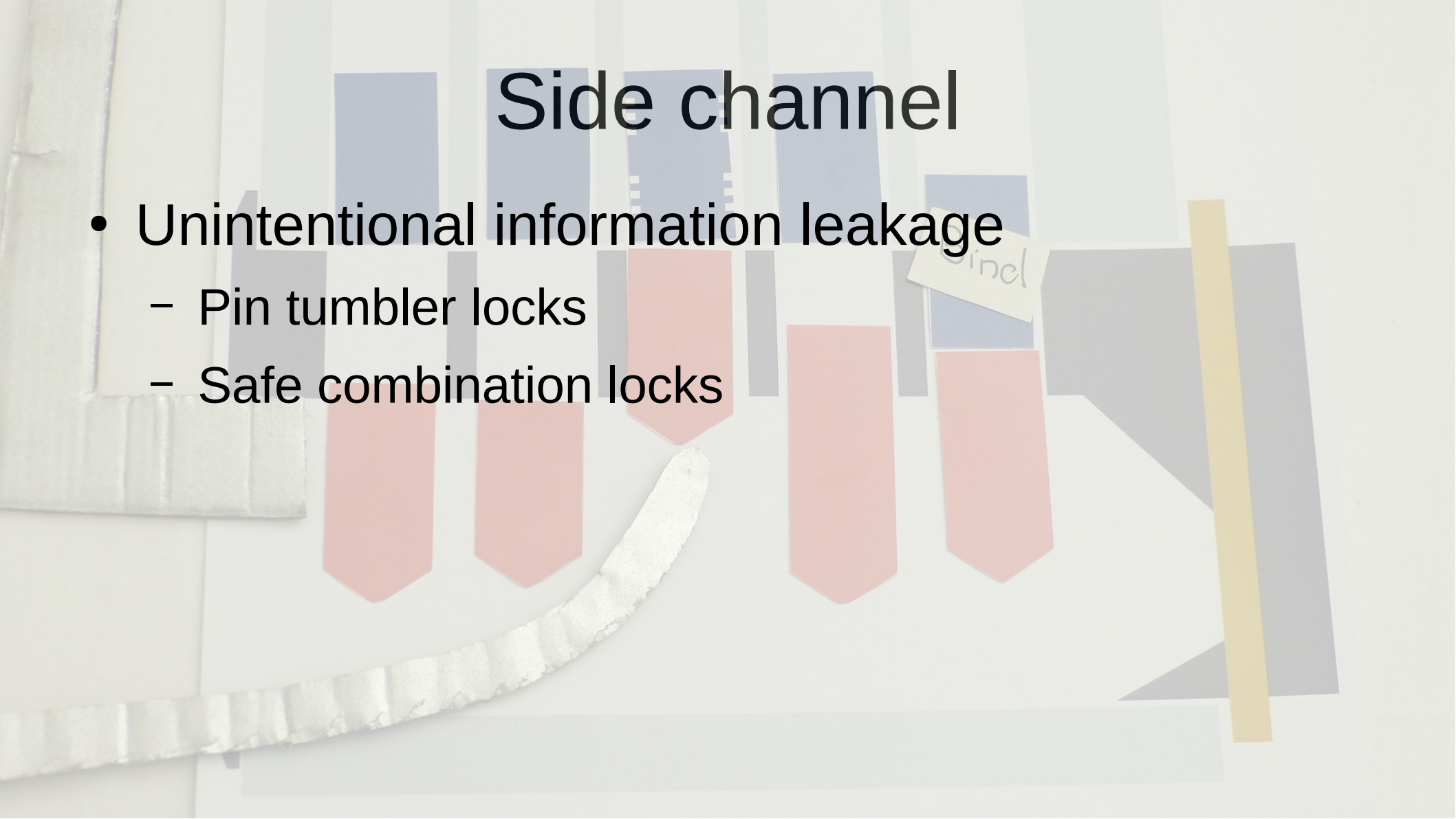
May Contain Hackers 2022

What if locks could talk; what stories would they tell?

- Talking with locks?
- History
- Side channels

Side channel

- Unintentional information leakage
  - Pin tumbler locks
  - Safe combination locks



Follow

Jan-Willem CCX

@jwrm22

Nerd, Board member of TOOOL, Electrical engineer, Hardware Hacker #Cyber

The Open Organisation Of Lockpickers

- Started in 2002
- 50 members in the Netherlands
- Weekly lockpicking meetings
- Lockpicking village @ Clairvoyance

The Open Organisation Of Lockpickers

Rules of Lockpicking

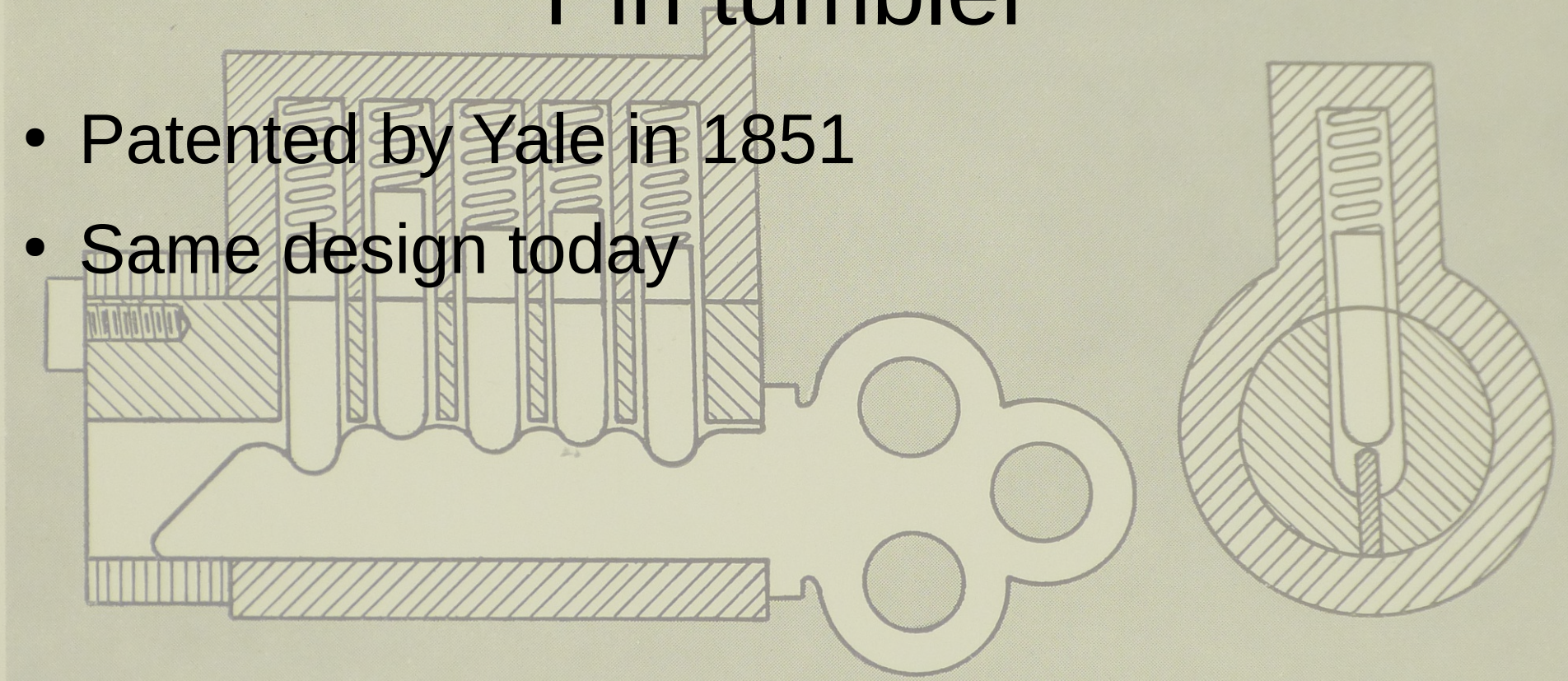
- Pick your own locks.
- When locks are in use, find another to pick.

Rules of Lockpicking

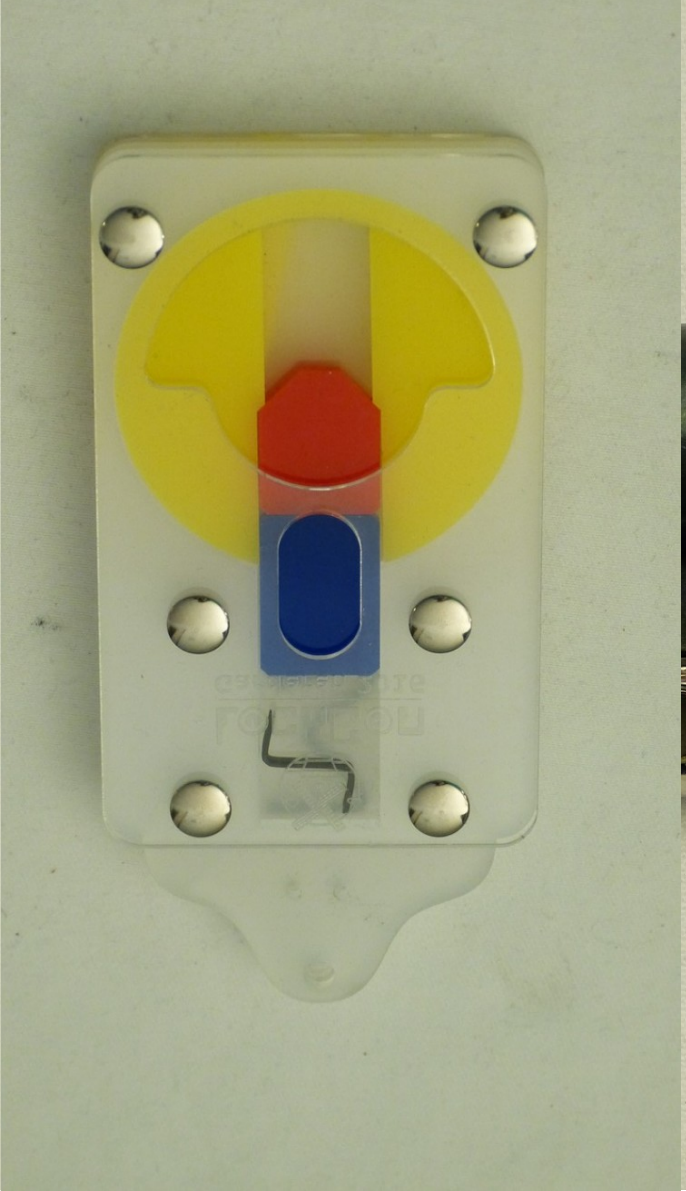
- In short:
  - Only pick locks you own,
  - do not rely on and can afford to be without.

Pin tumbler

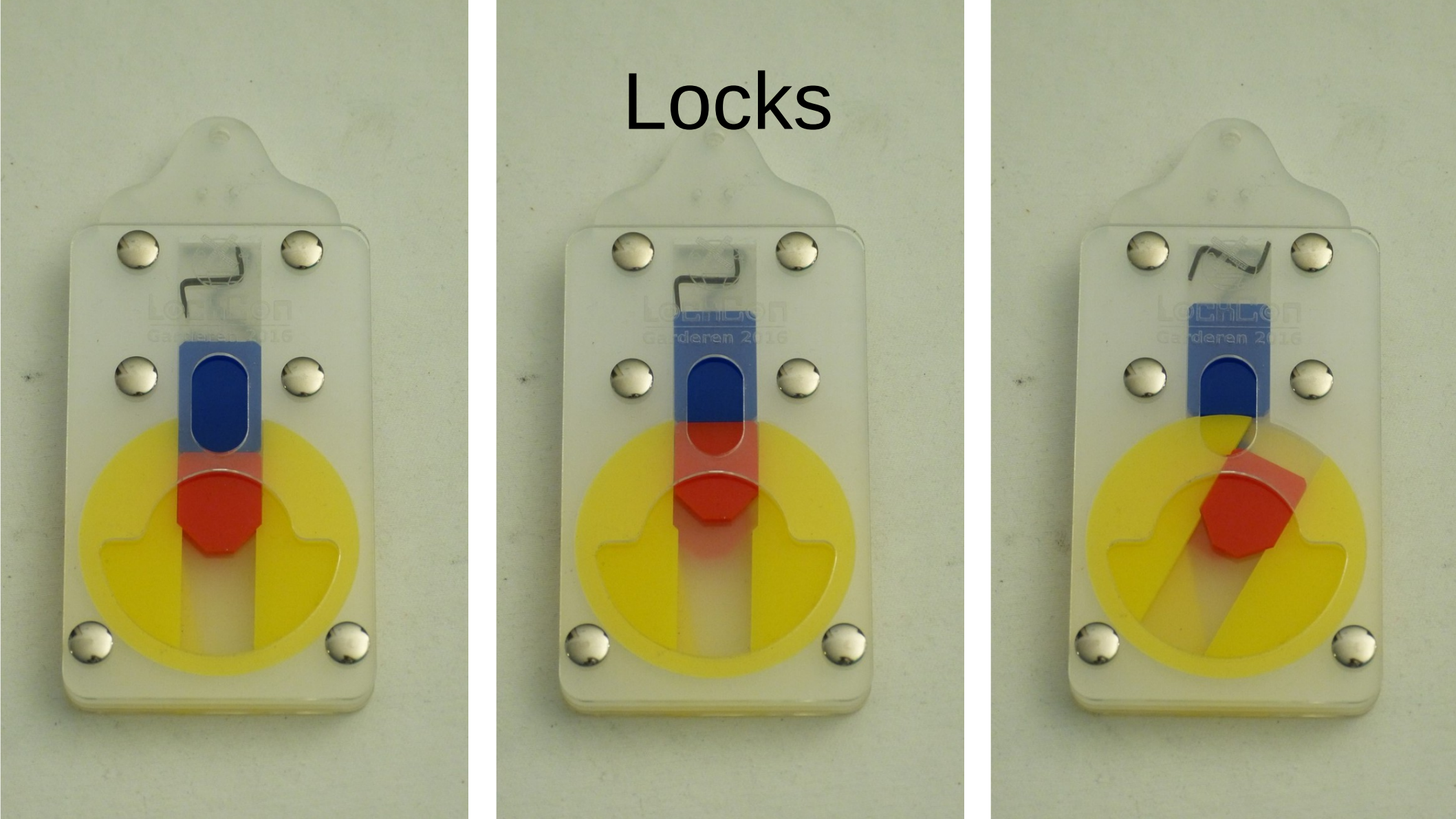
- Patented by Yale in 1851
- Same design today



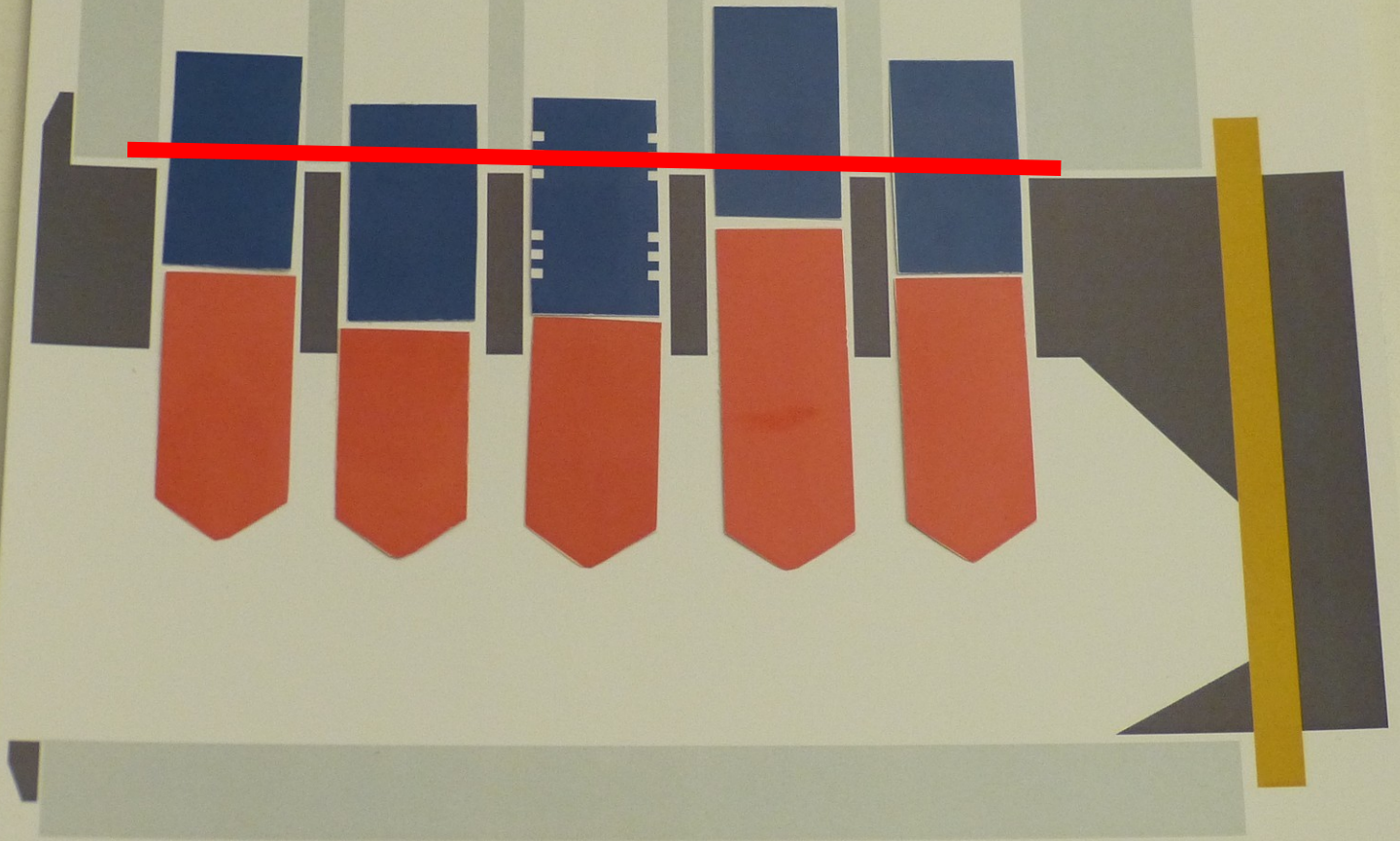
Orientation



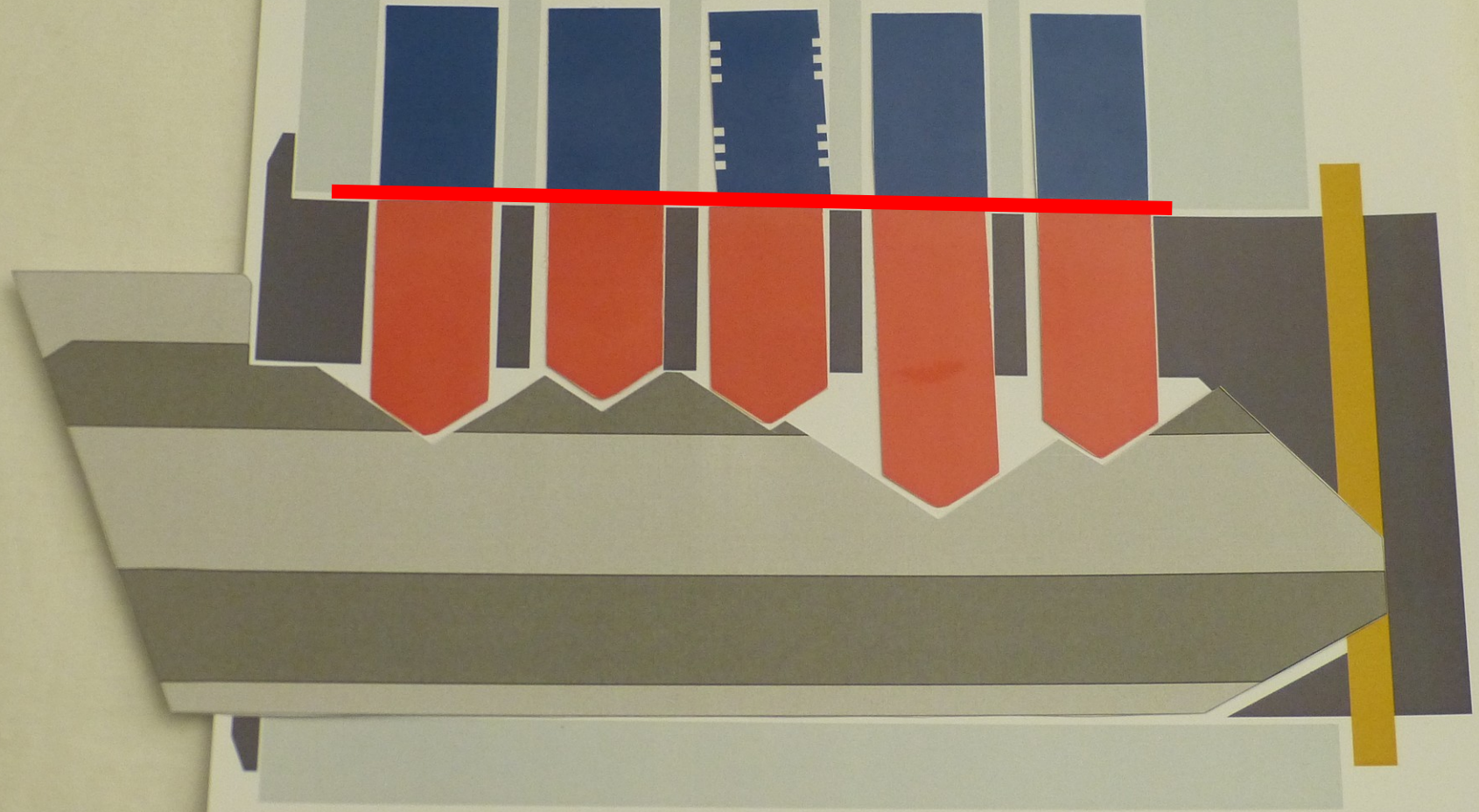
Locks



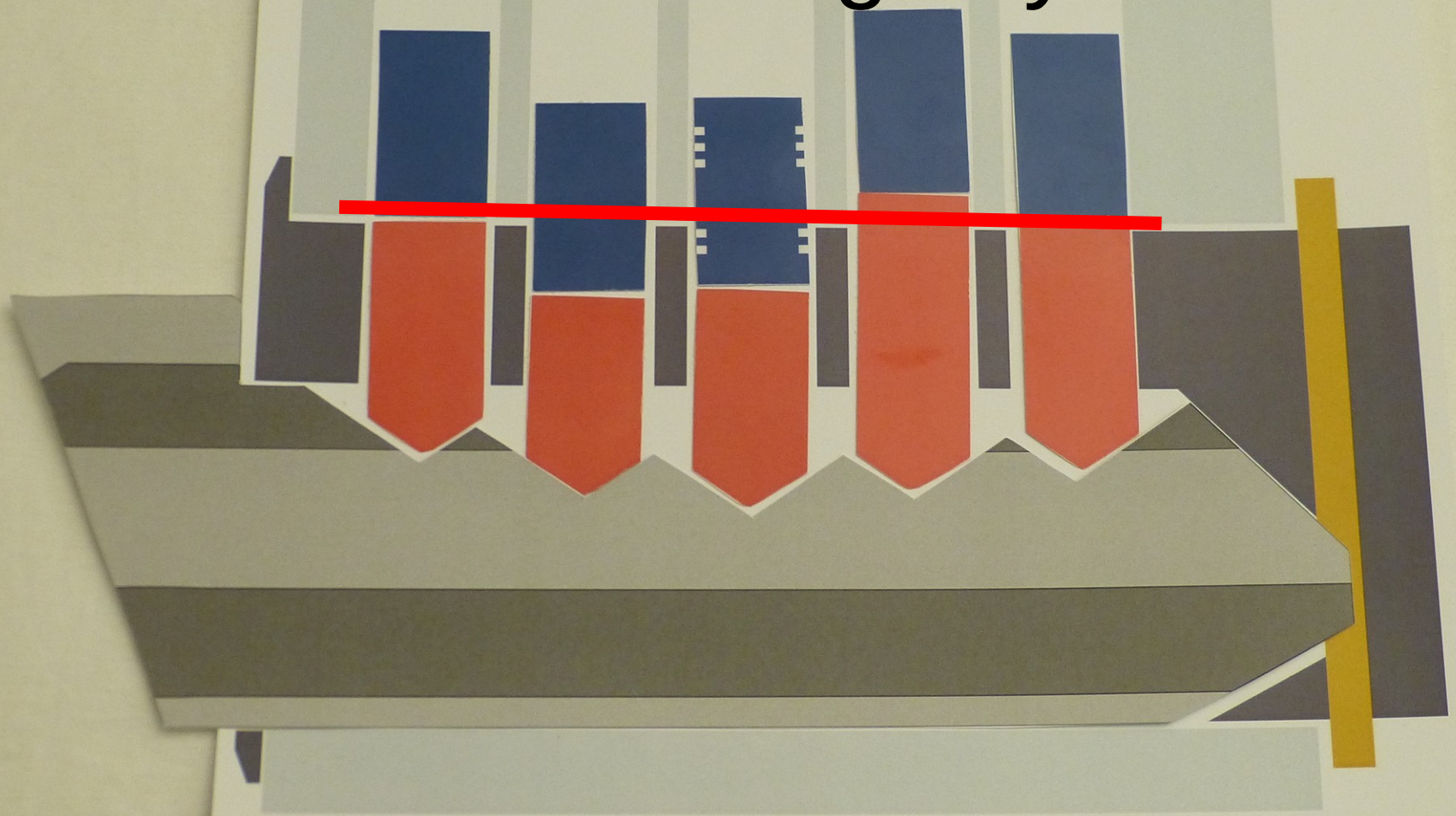
Without key



Correct key

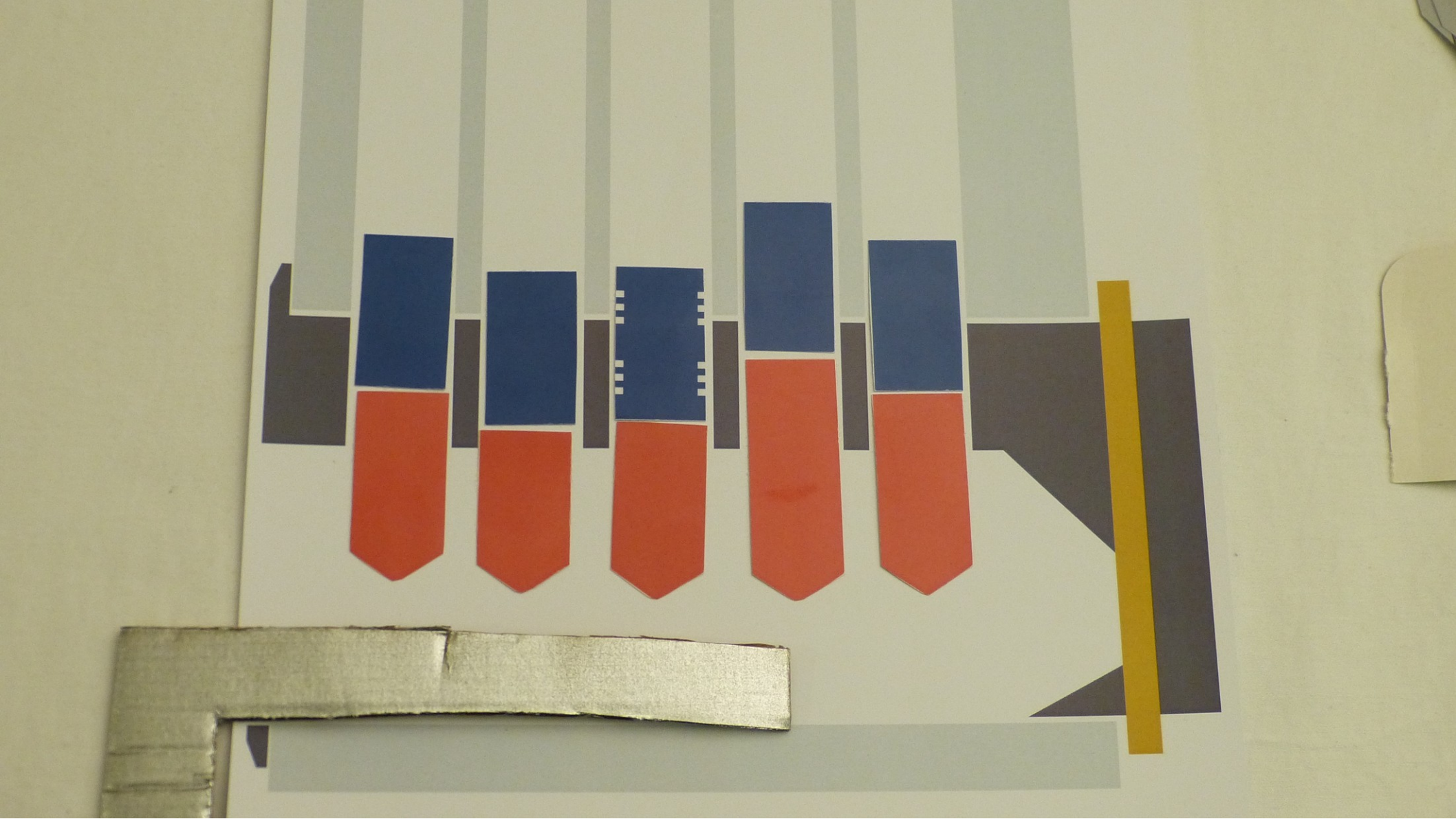


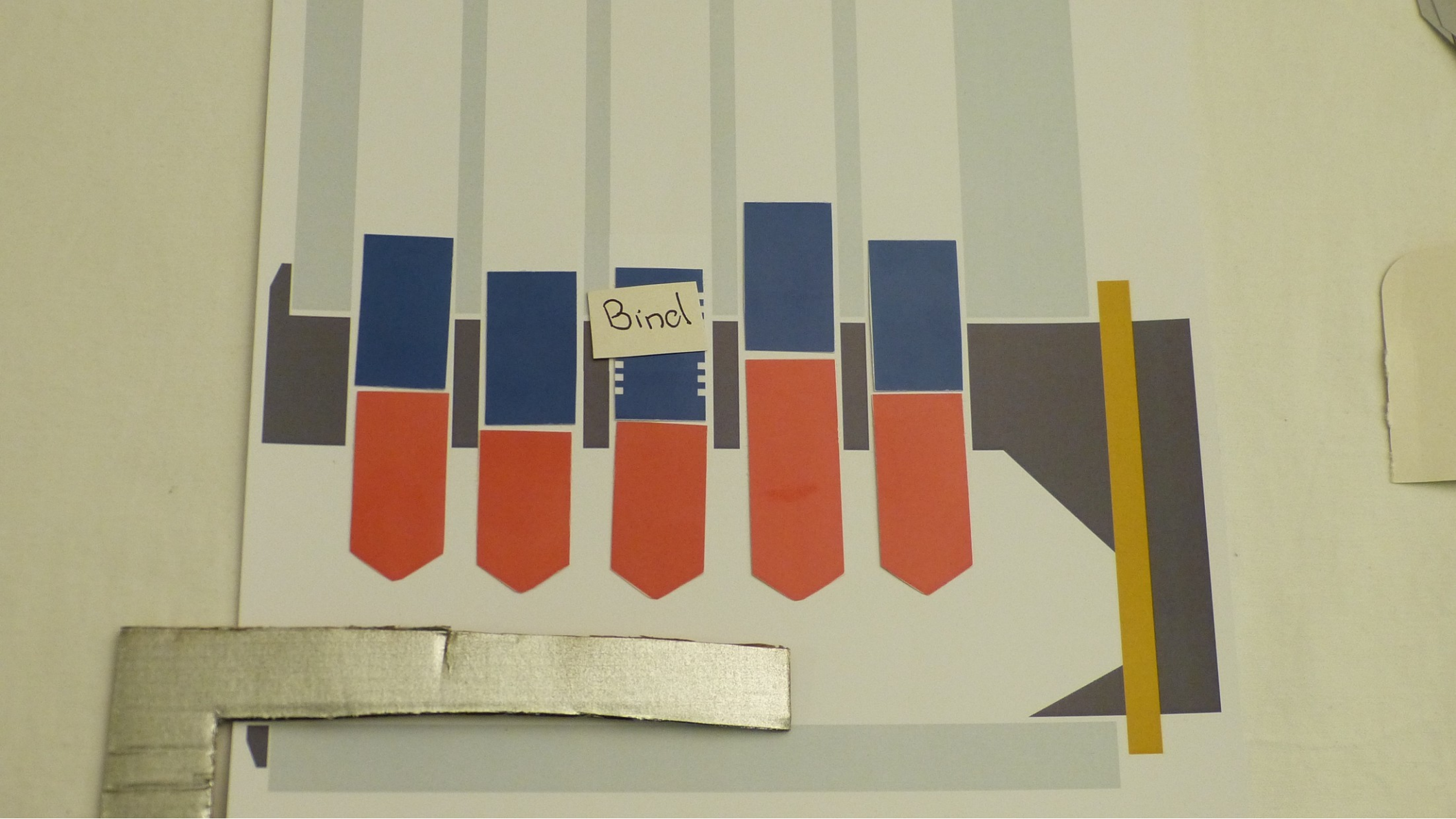
Wrong key

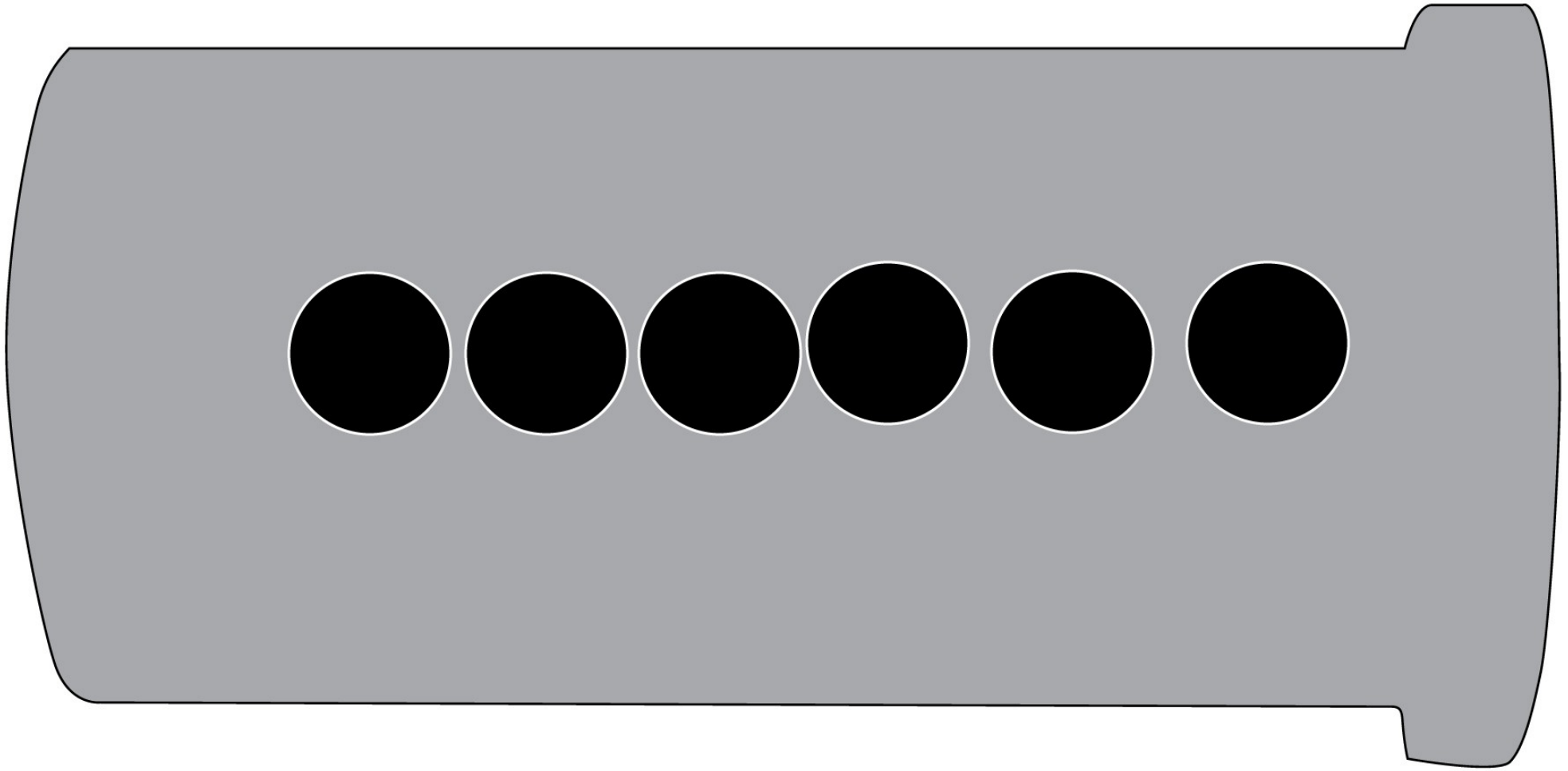


What are the side channels?

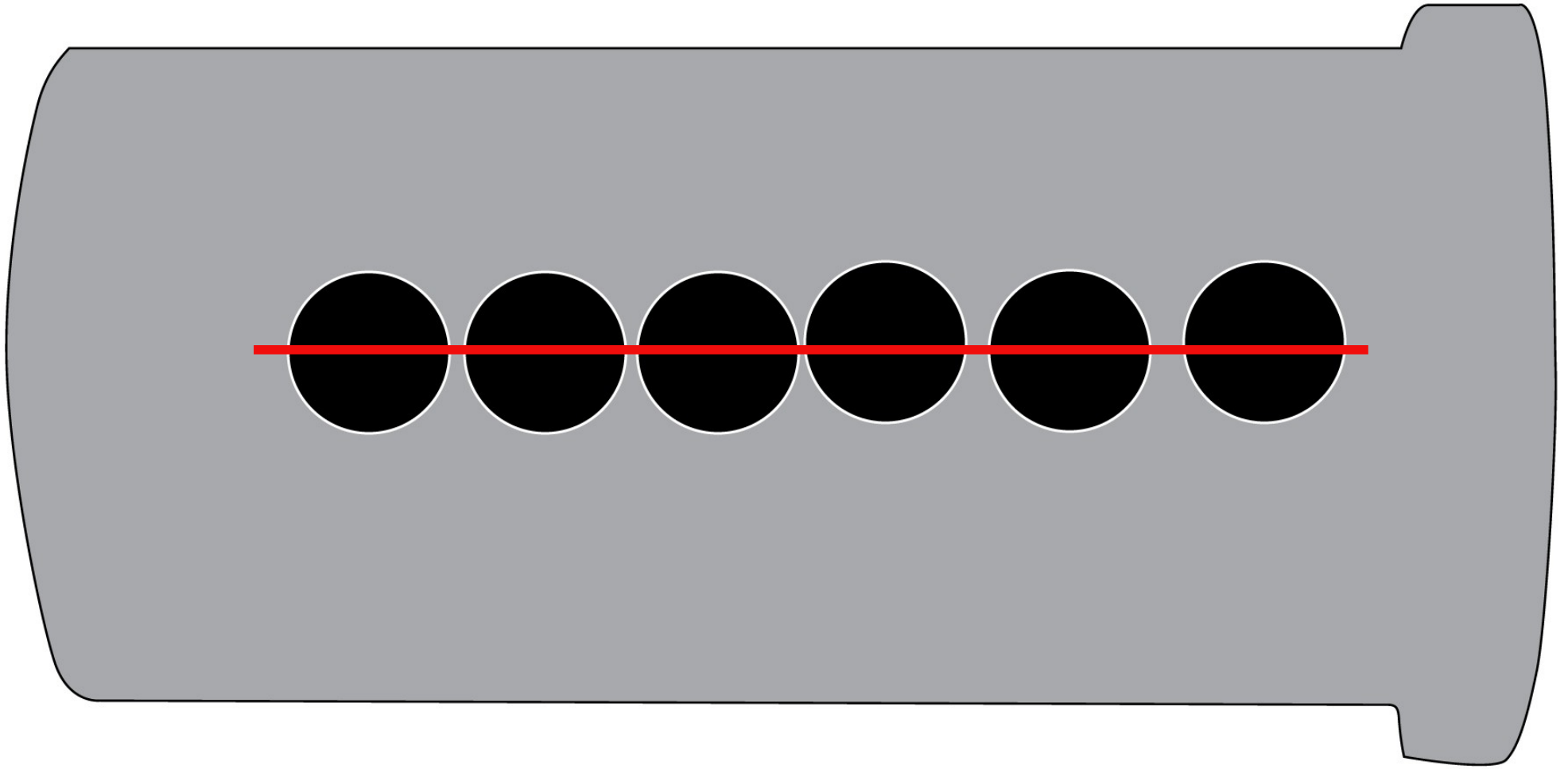
- Binding of the pins
- Rotation of the core
- ???



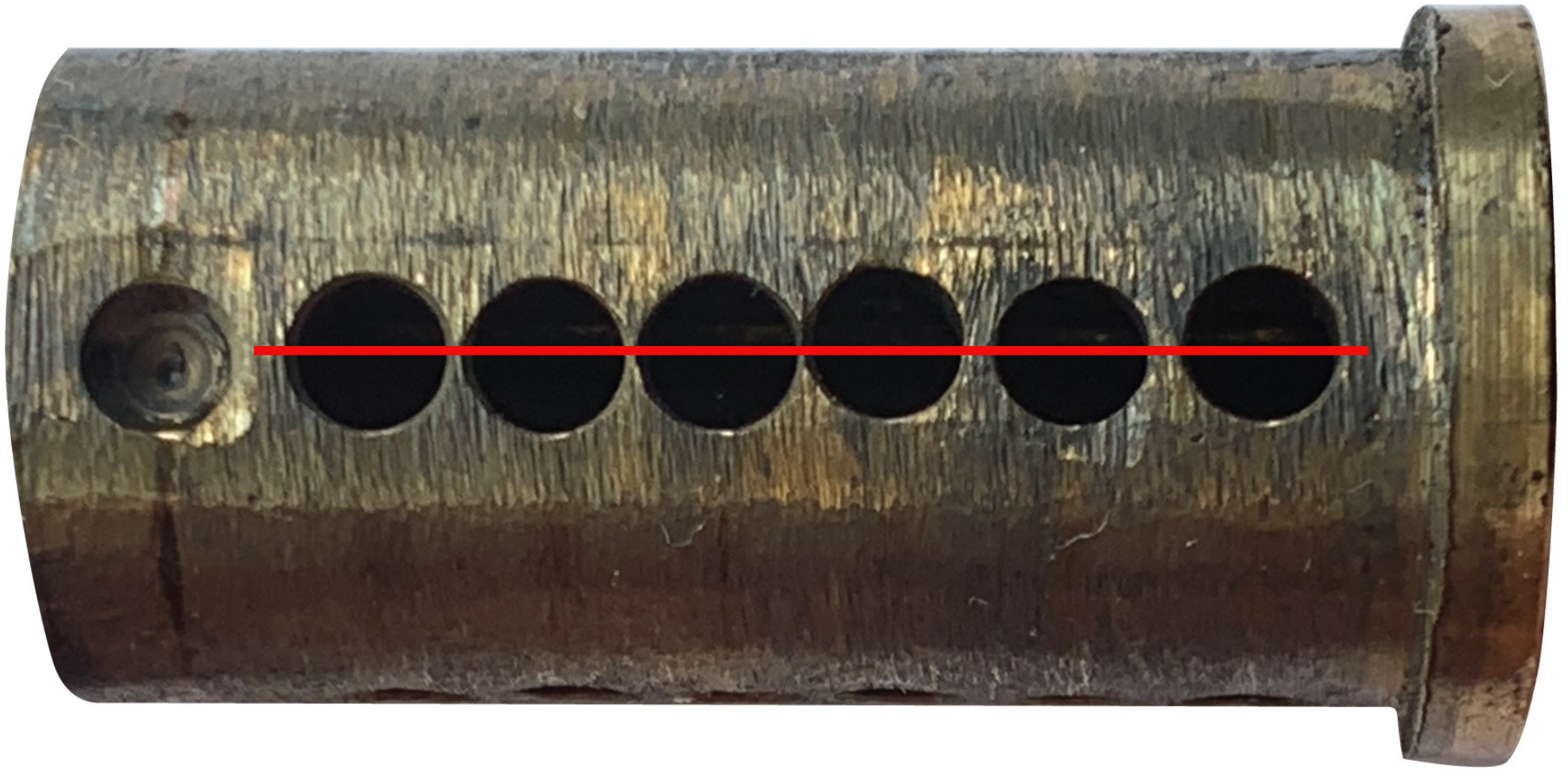

Bind



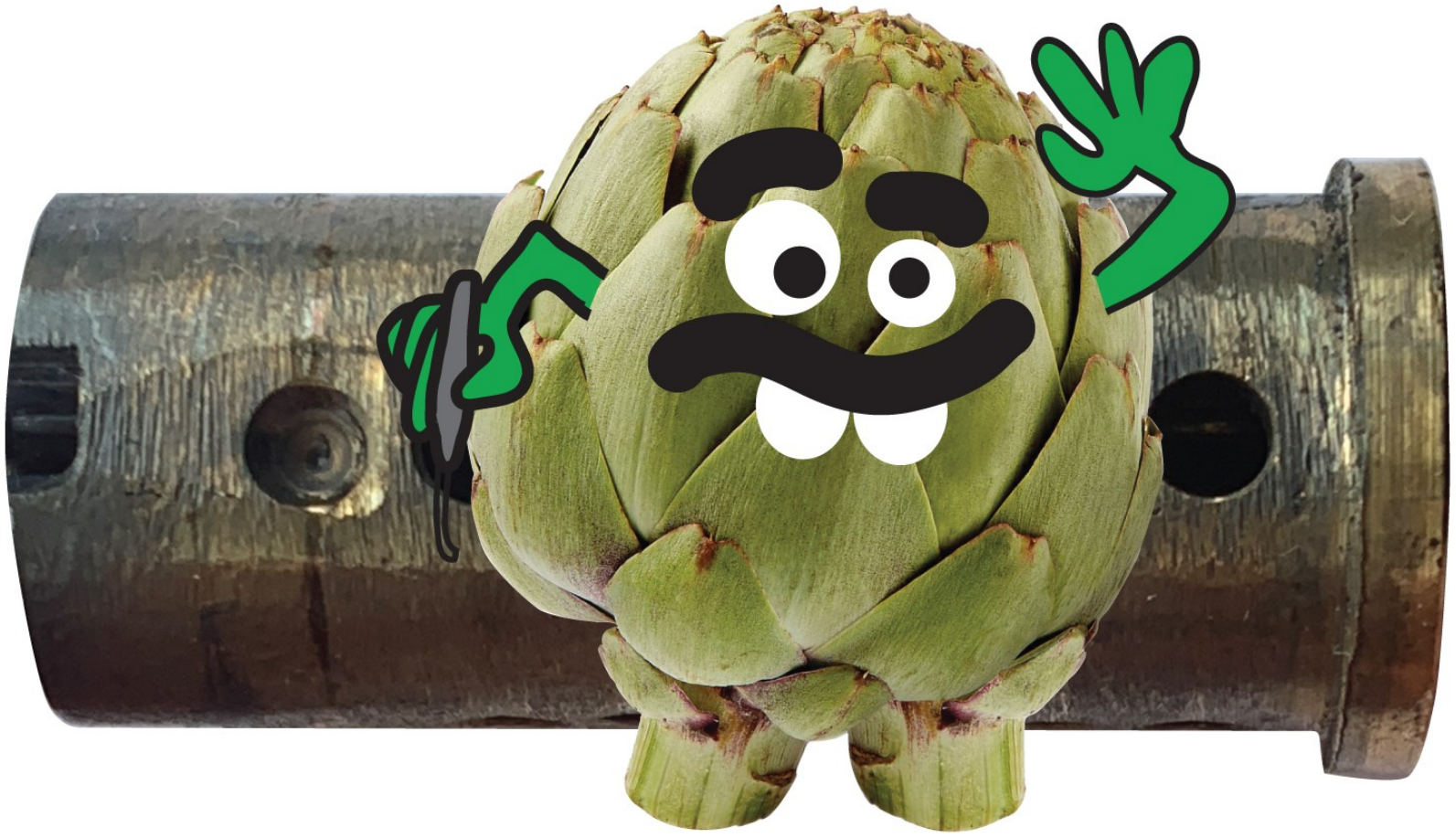
COURTESY ARTICHOKE2000



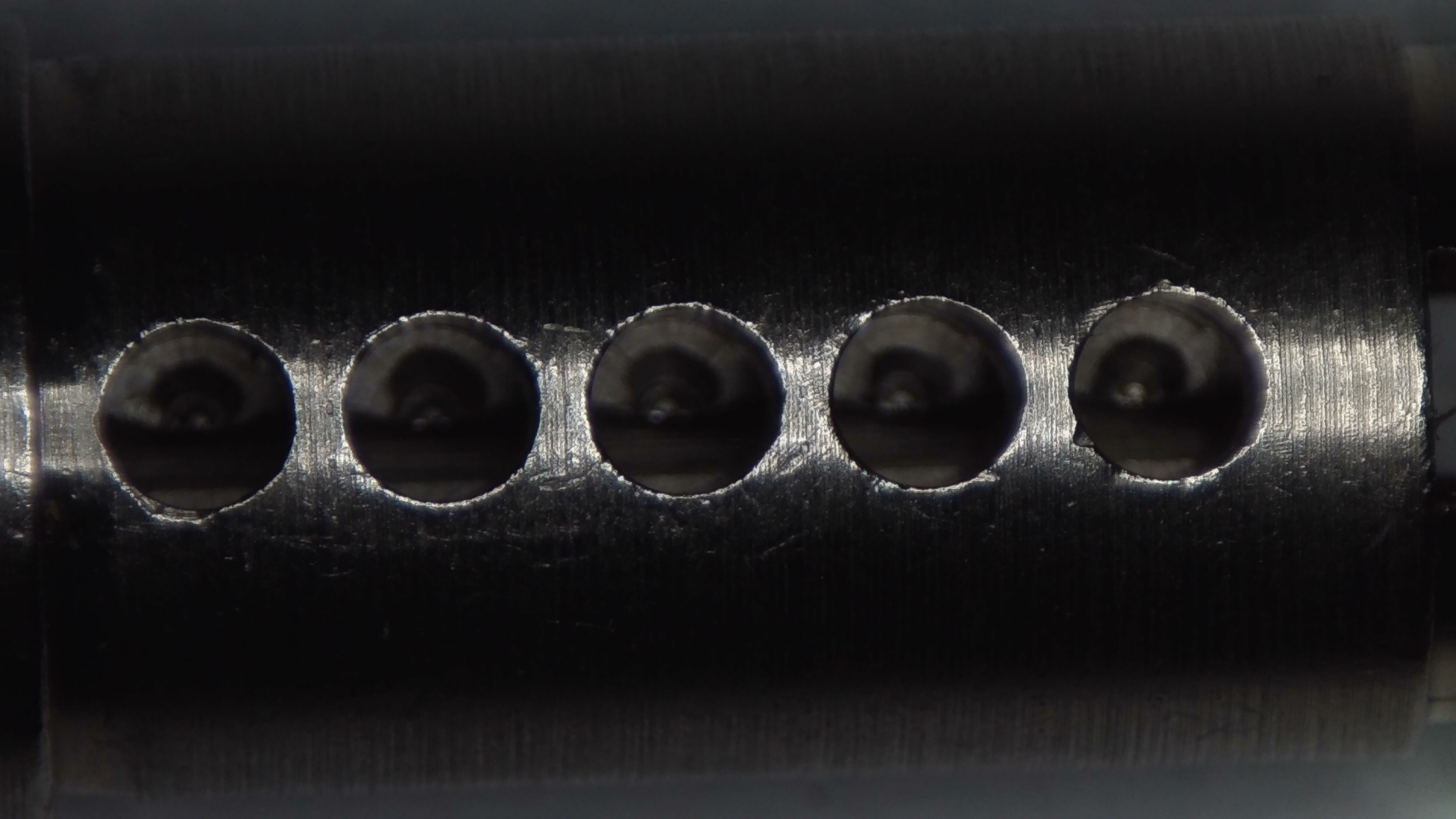
COURTESY ARTICHOKE2000

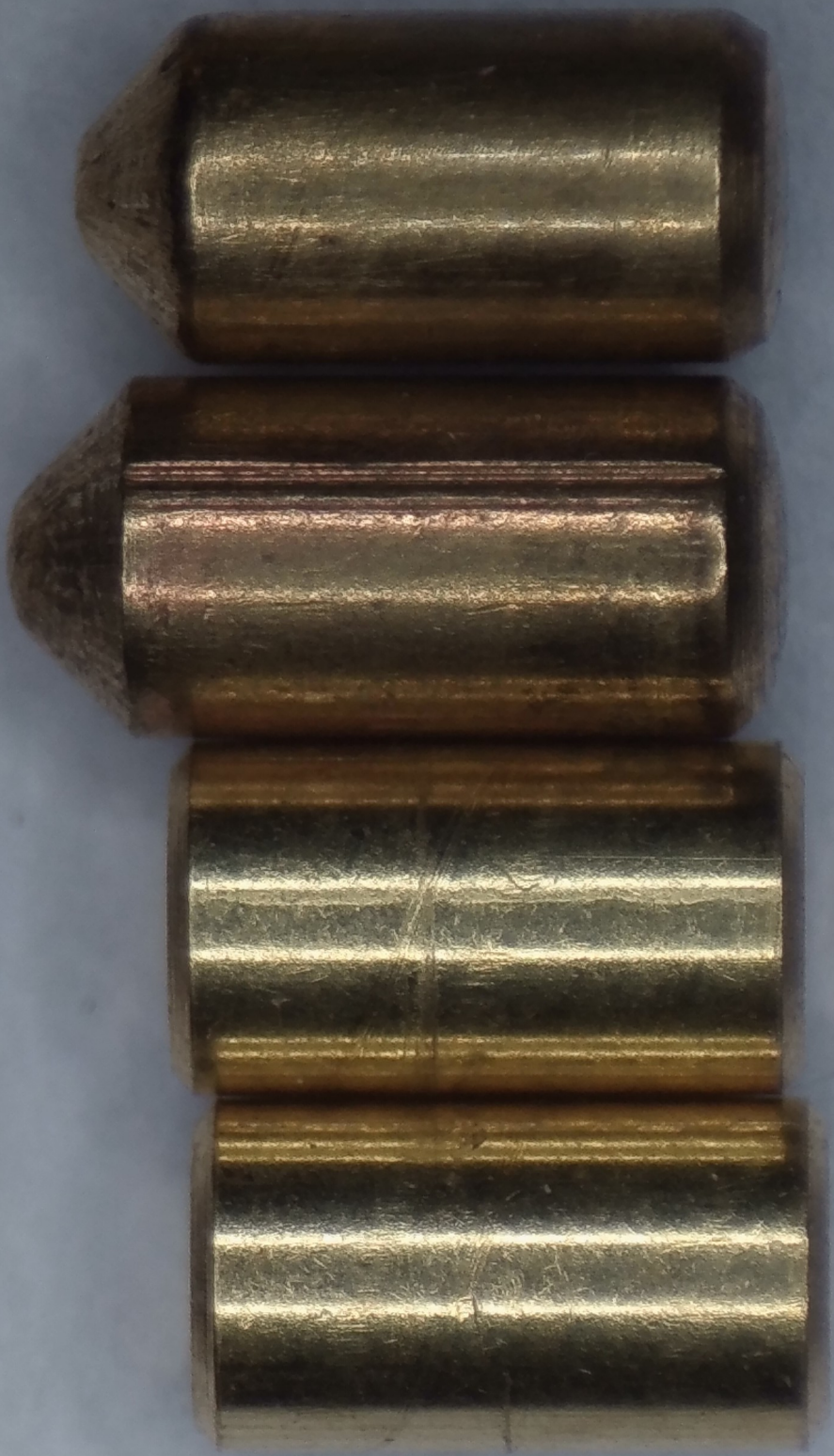


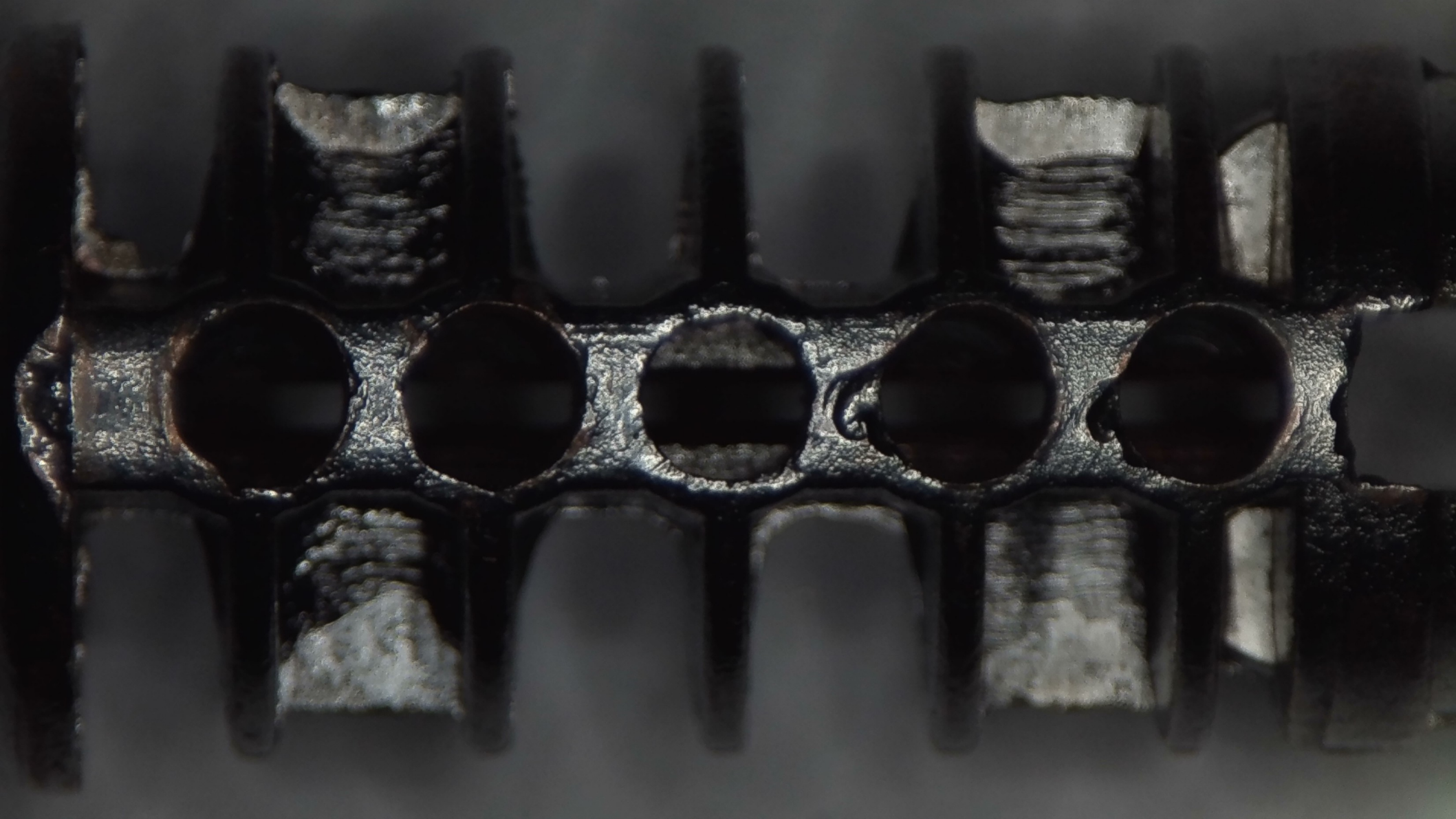
COURTESY ARTICHOKE2000



COURTESY ARTICHOKE2000







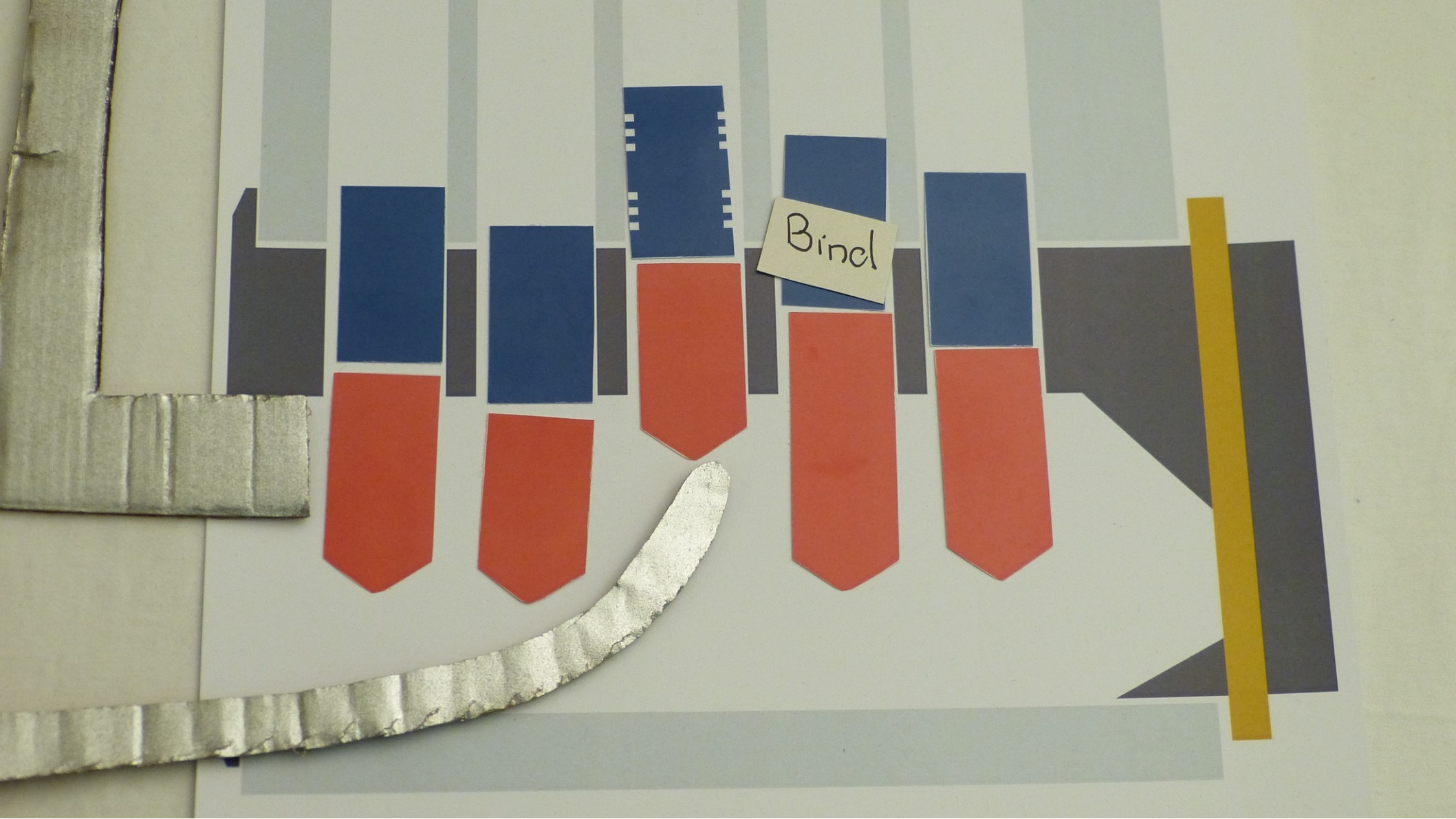
Lockpicking

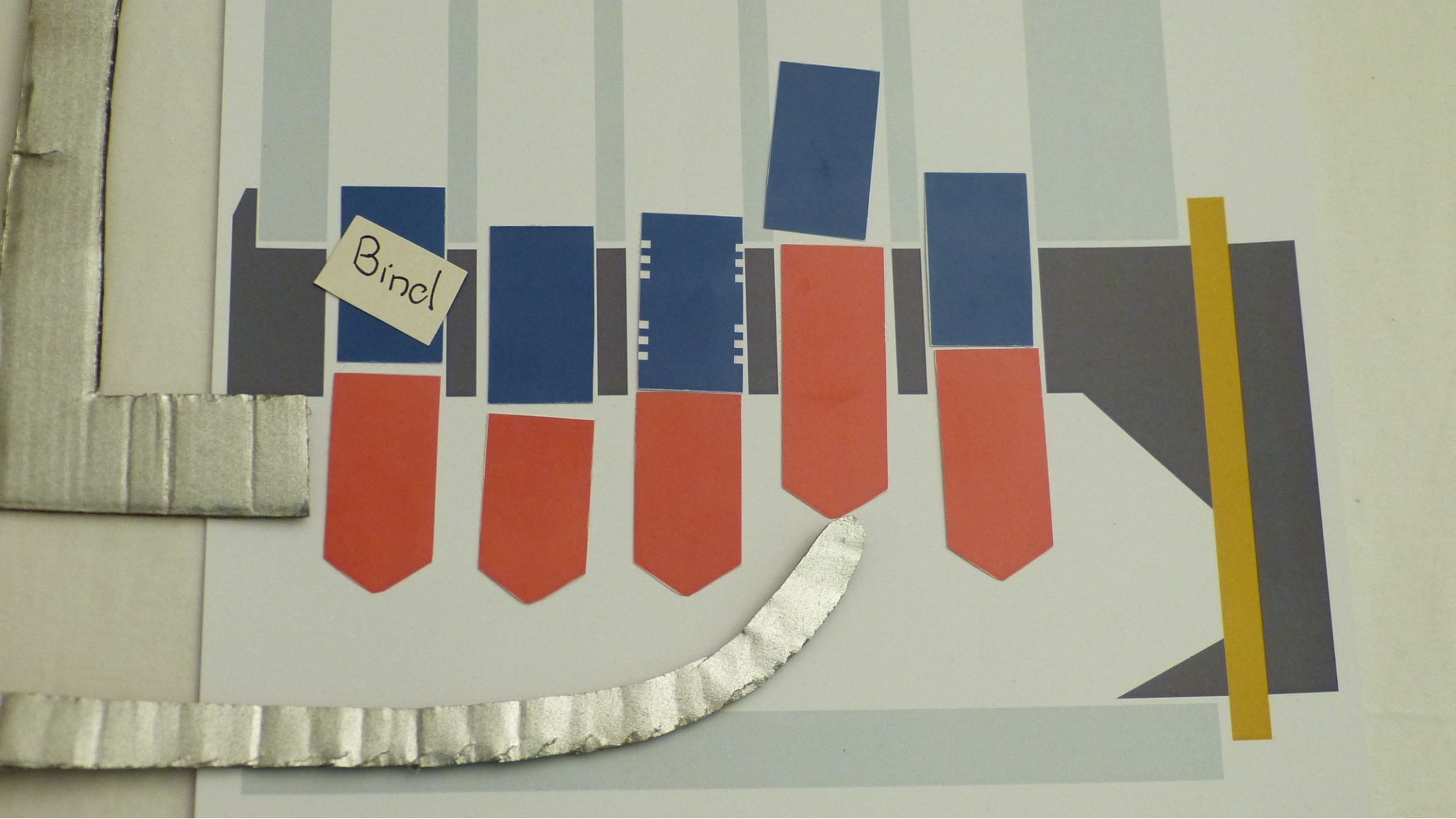

Bind


Bind


Bind

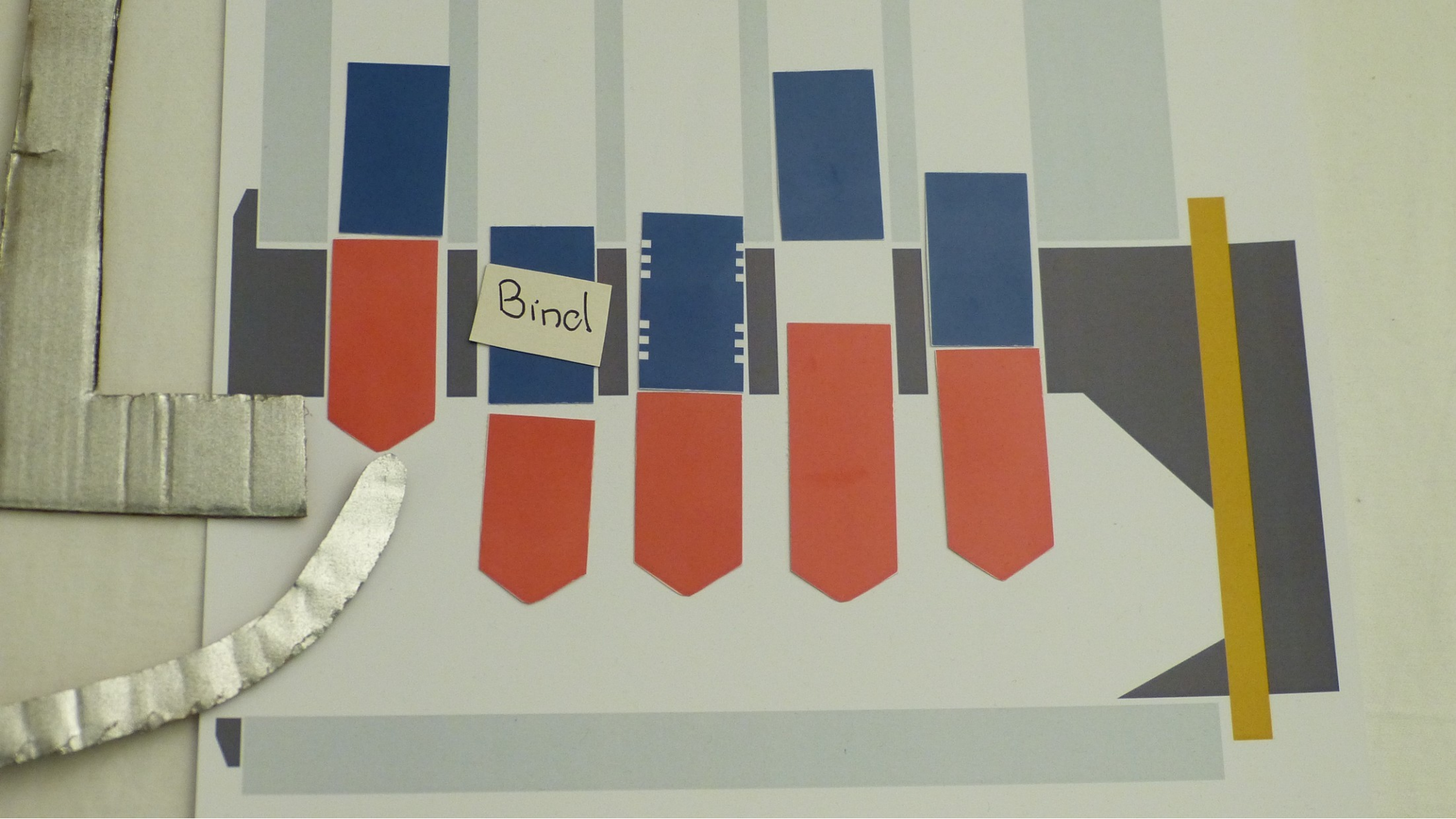

Bind

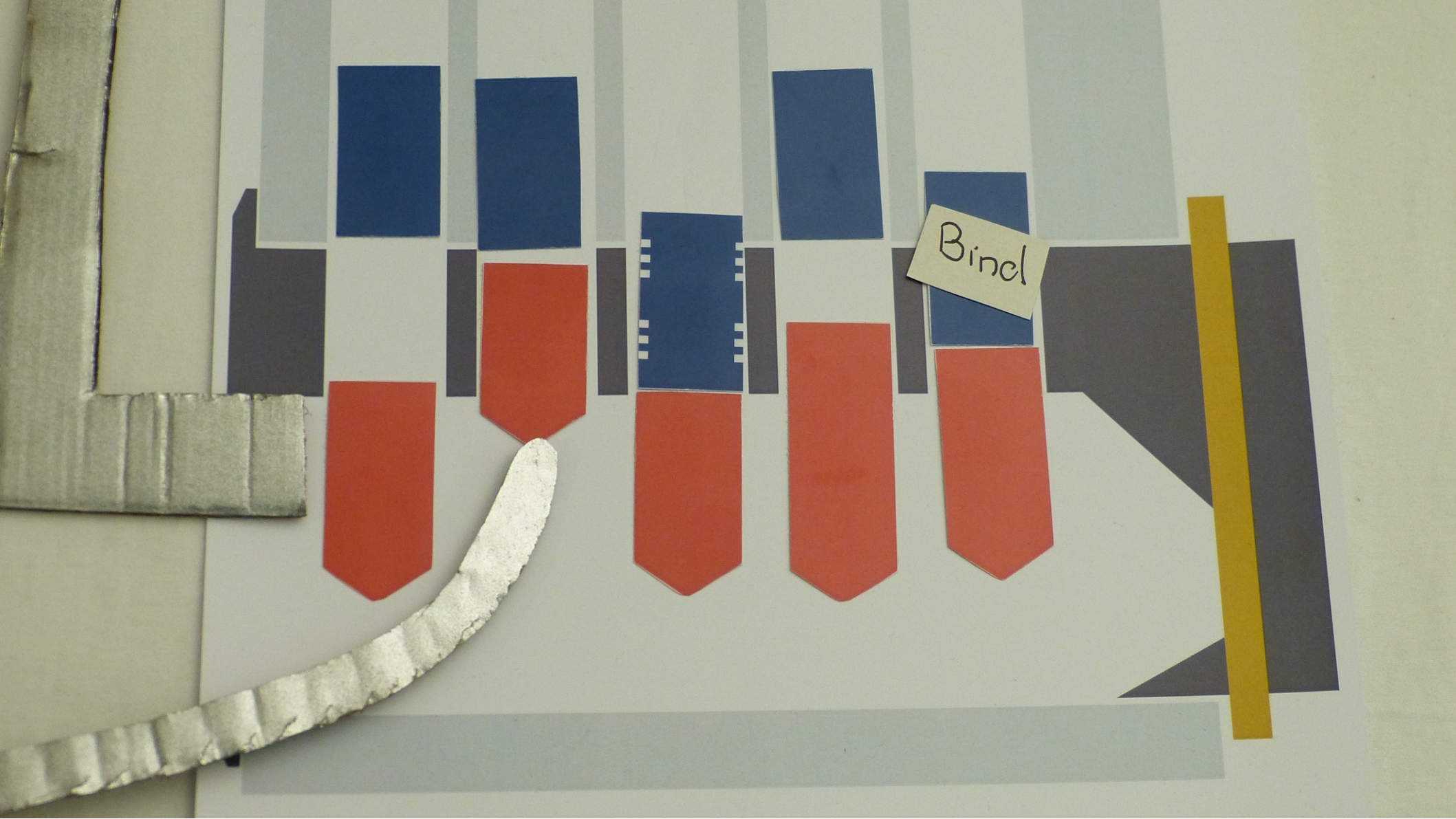

Bind

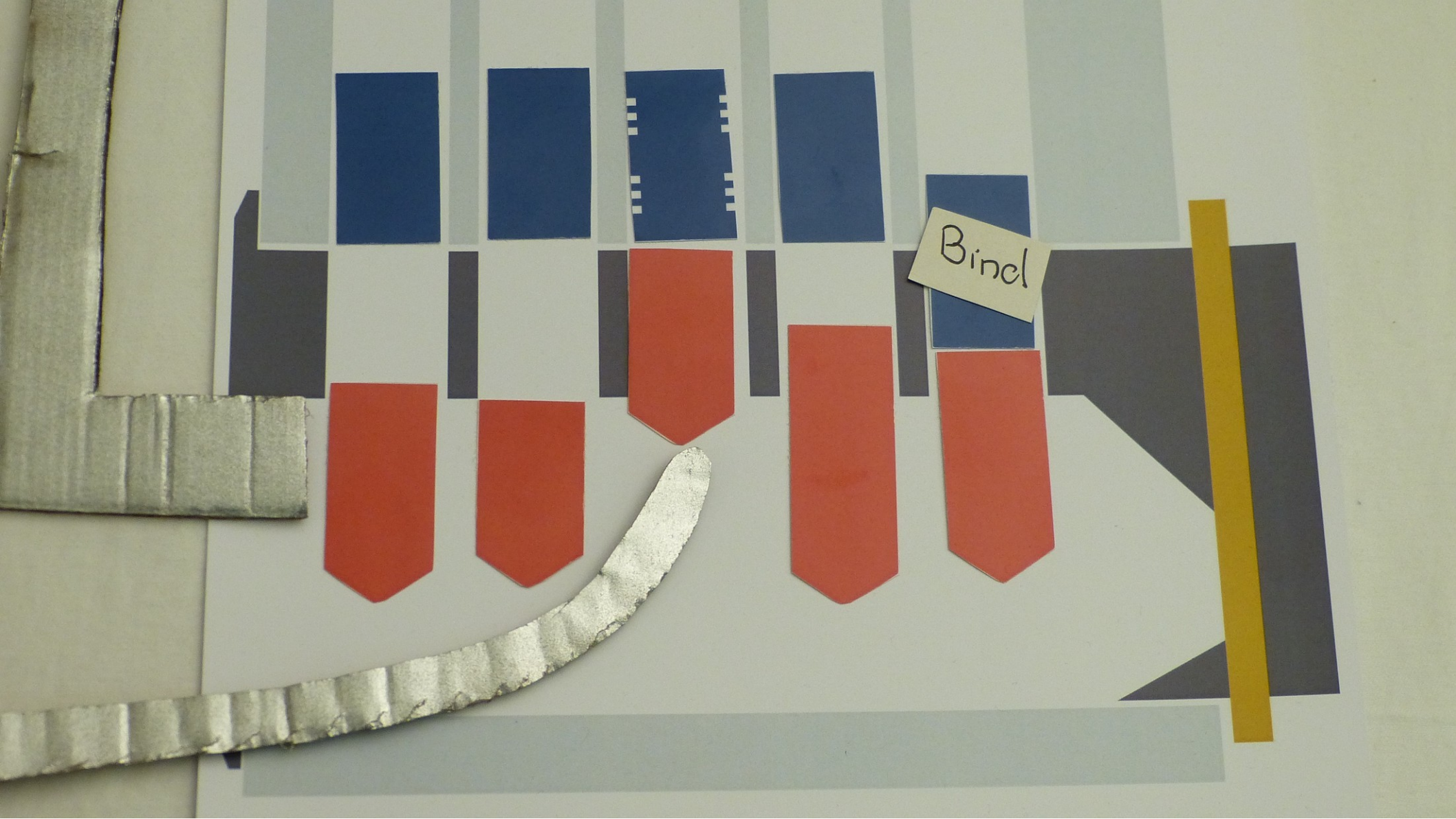

Bincl

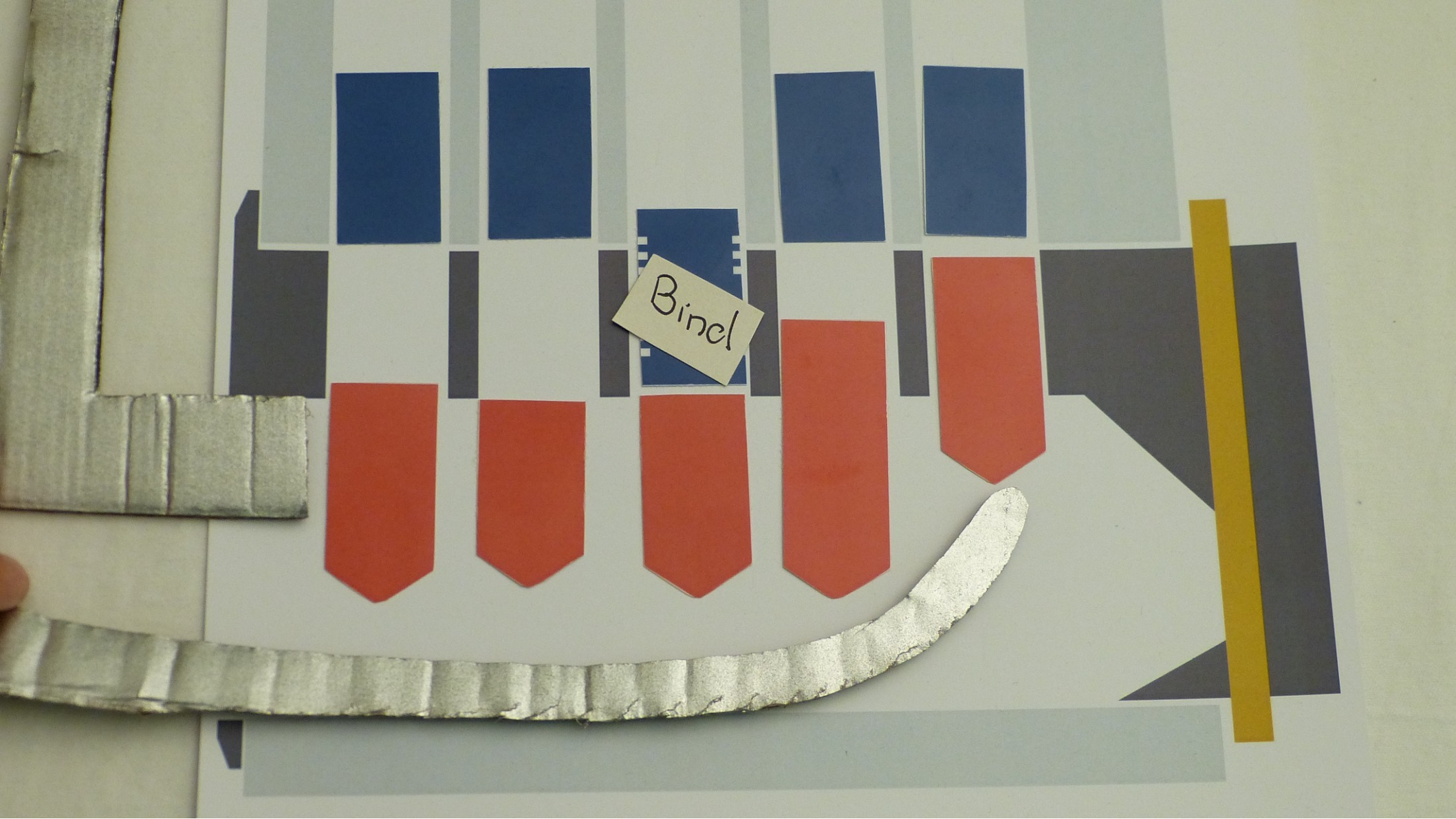

Binel

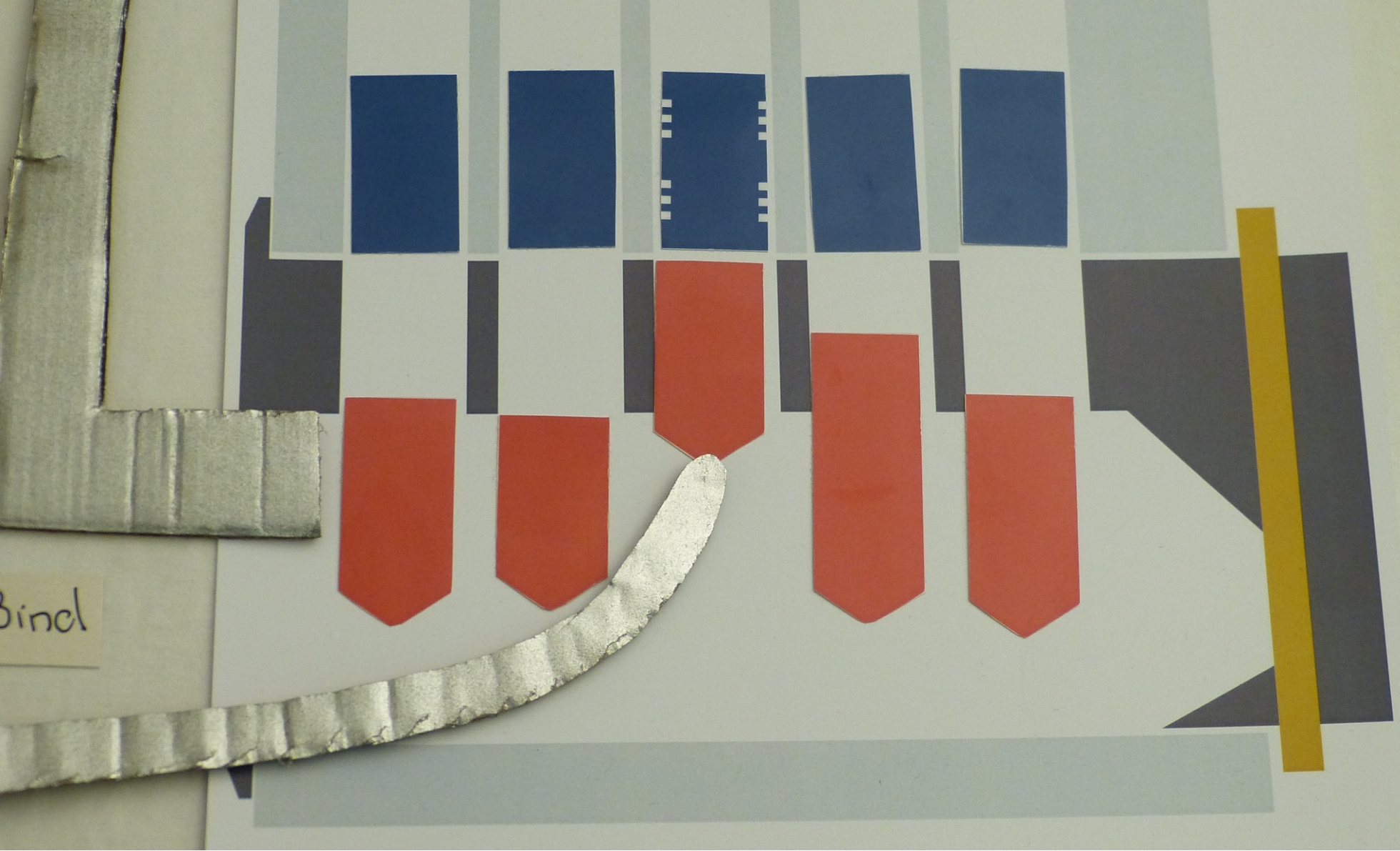

Binel


Bind


Binel


Bincl

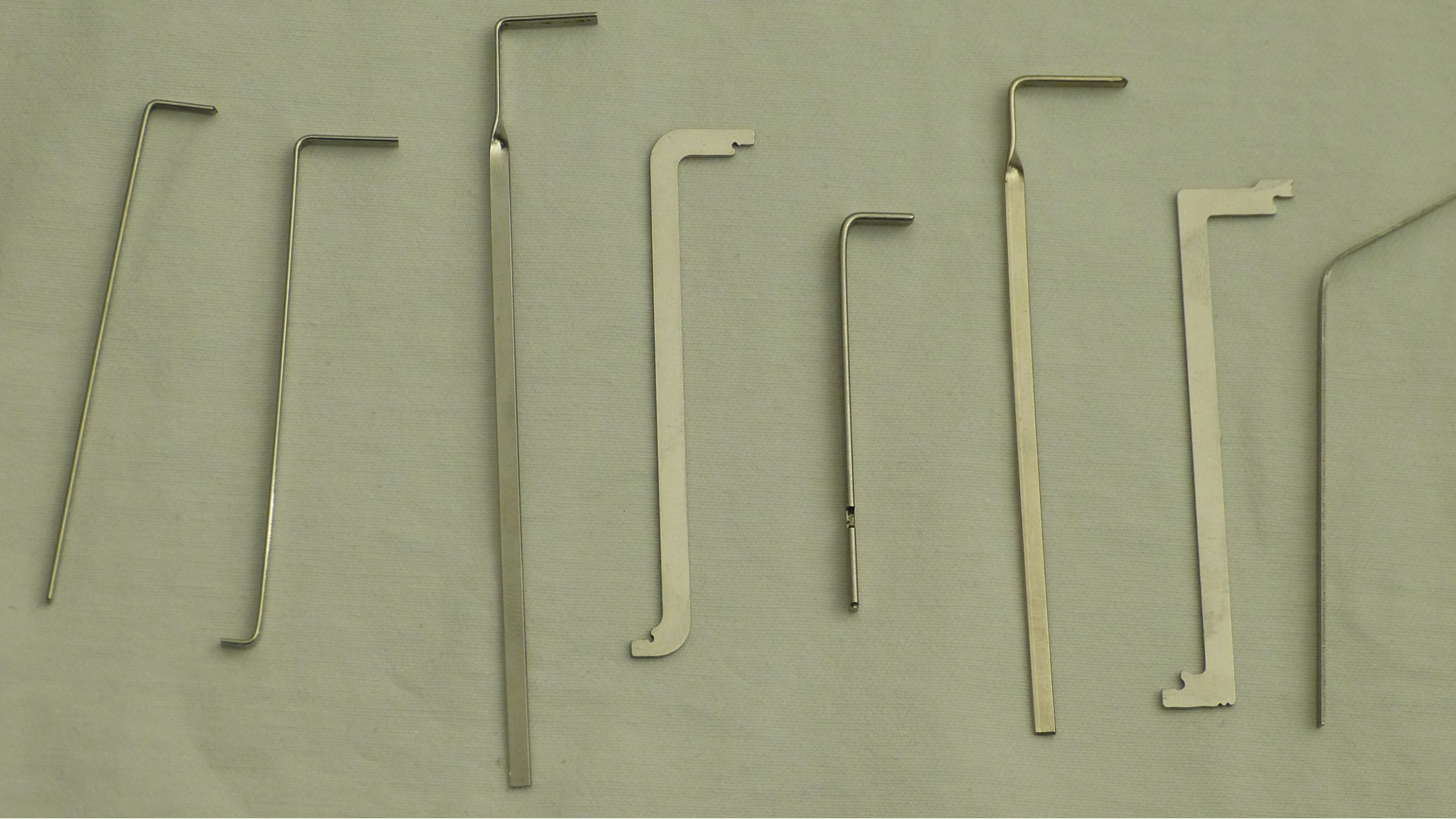

Binel

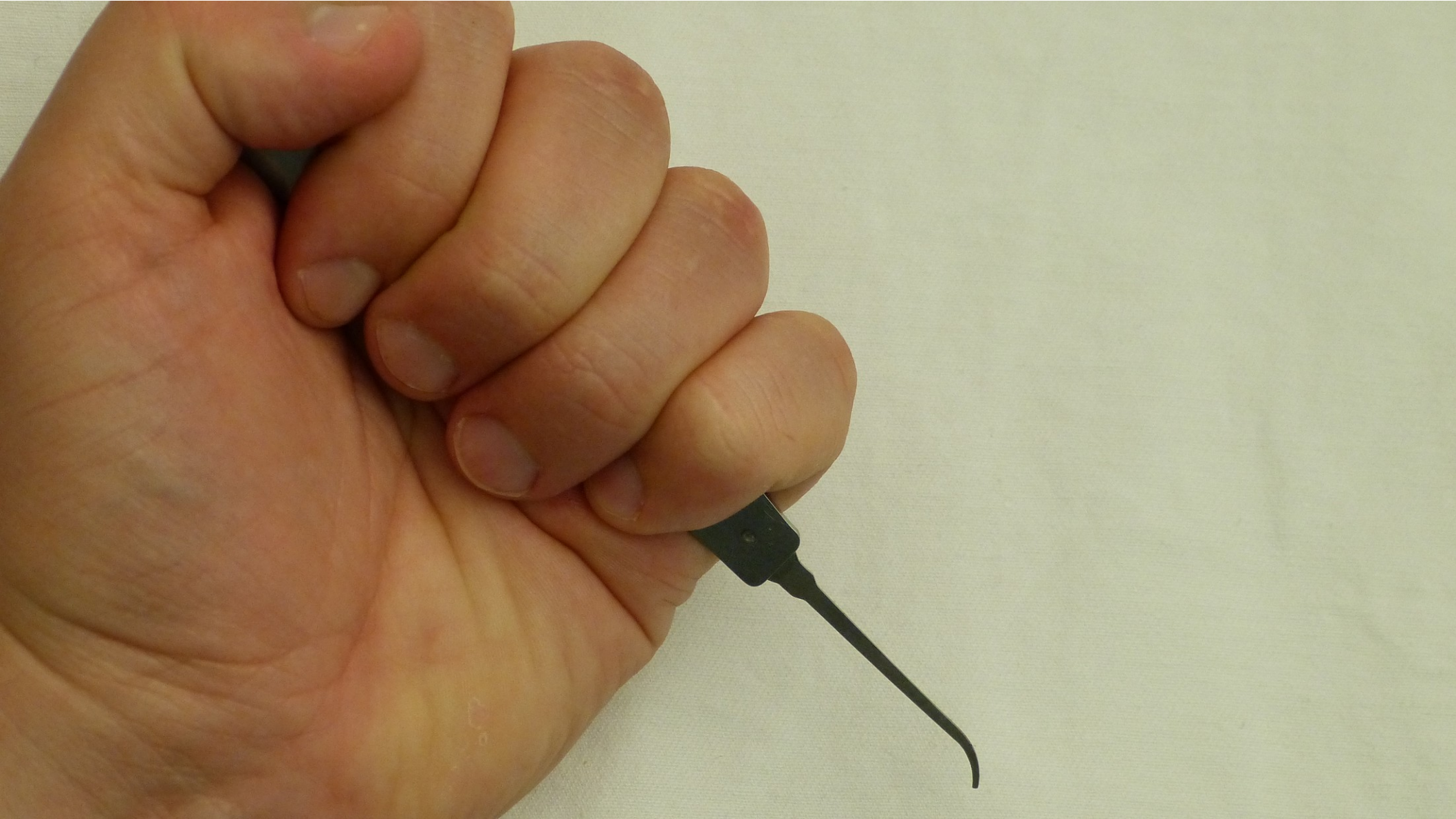

Bindl

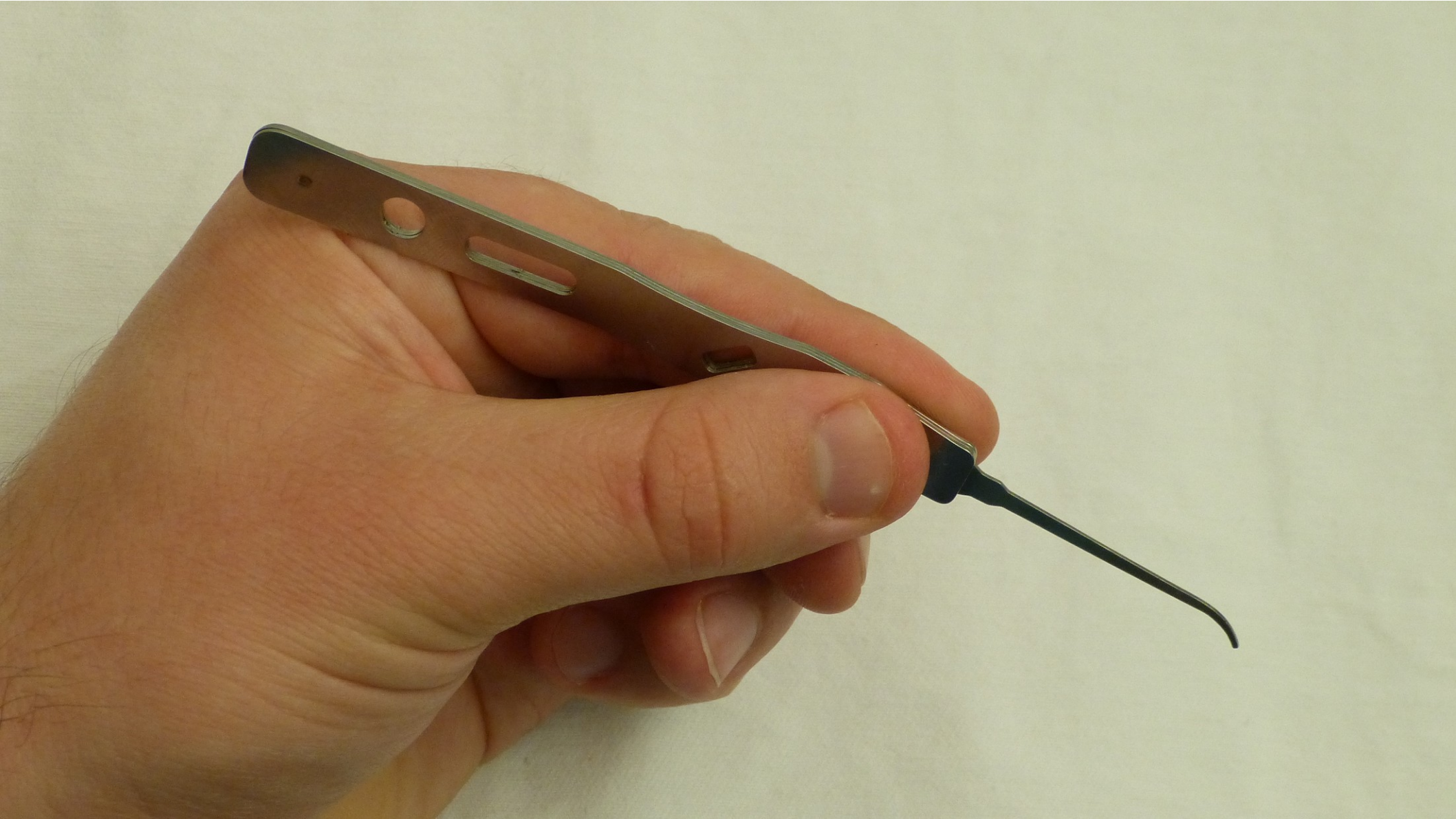

Bindl

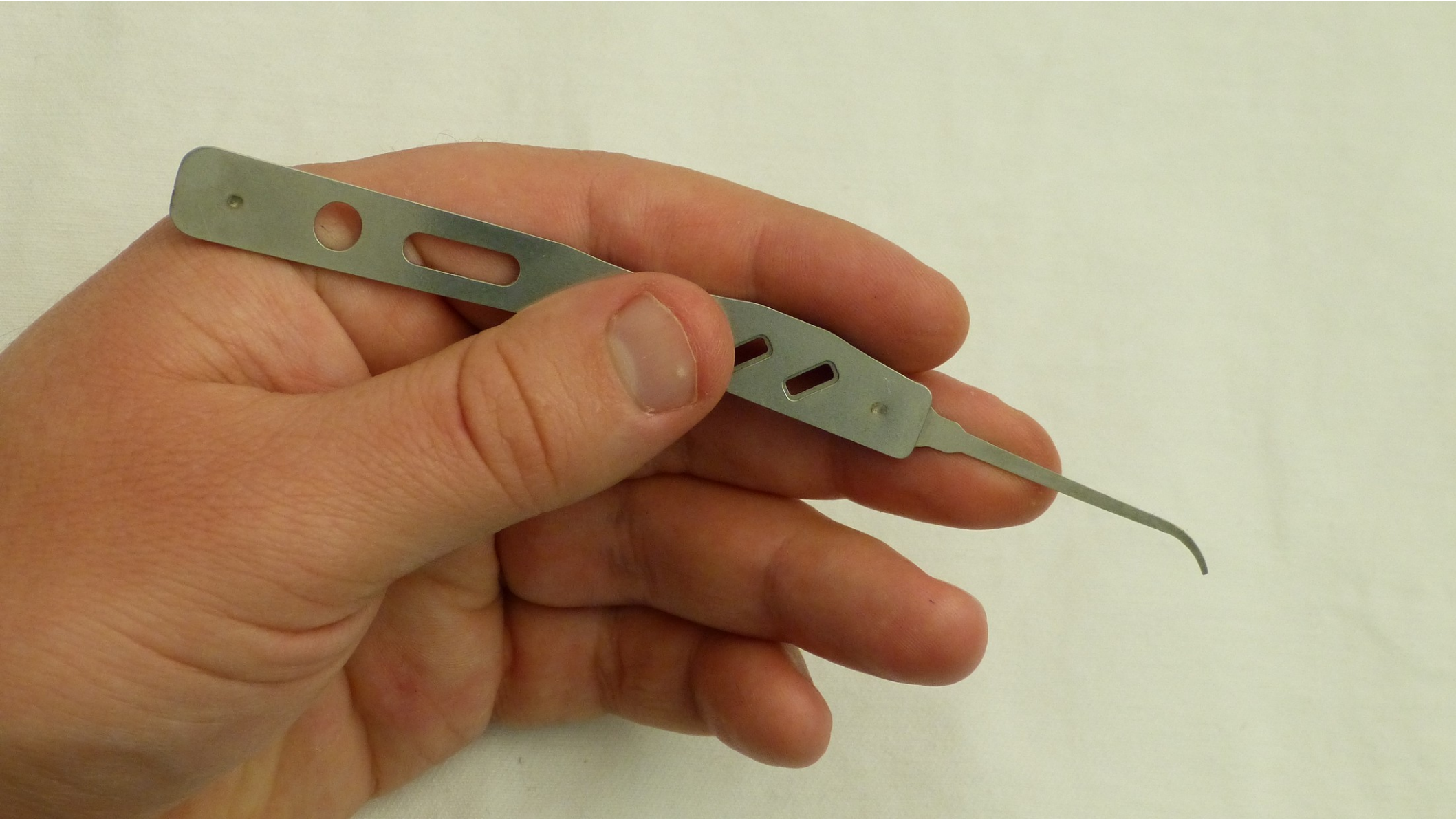

PN08
PN09

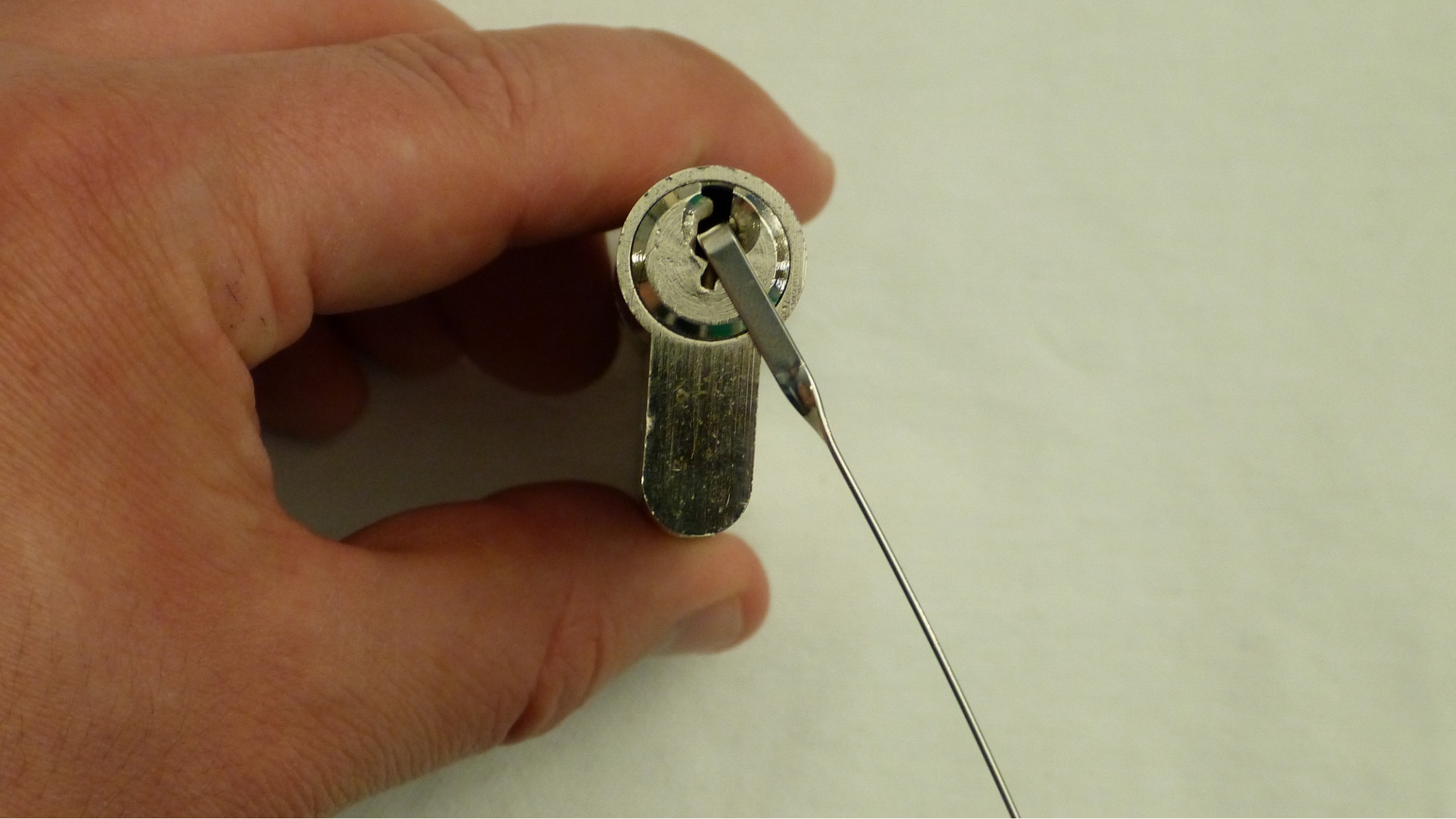

PN06
PETERSON
SOUTHORD MAX
SOUTHORD

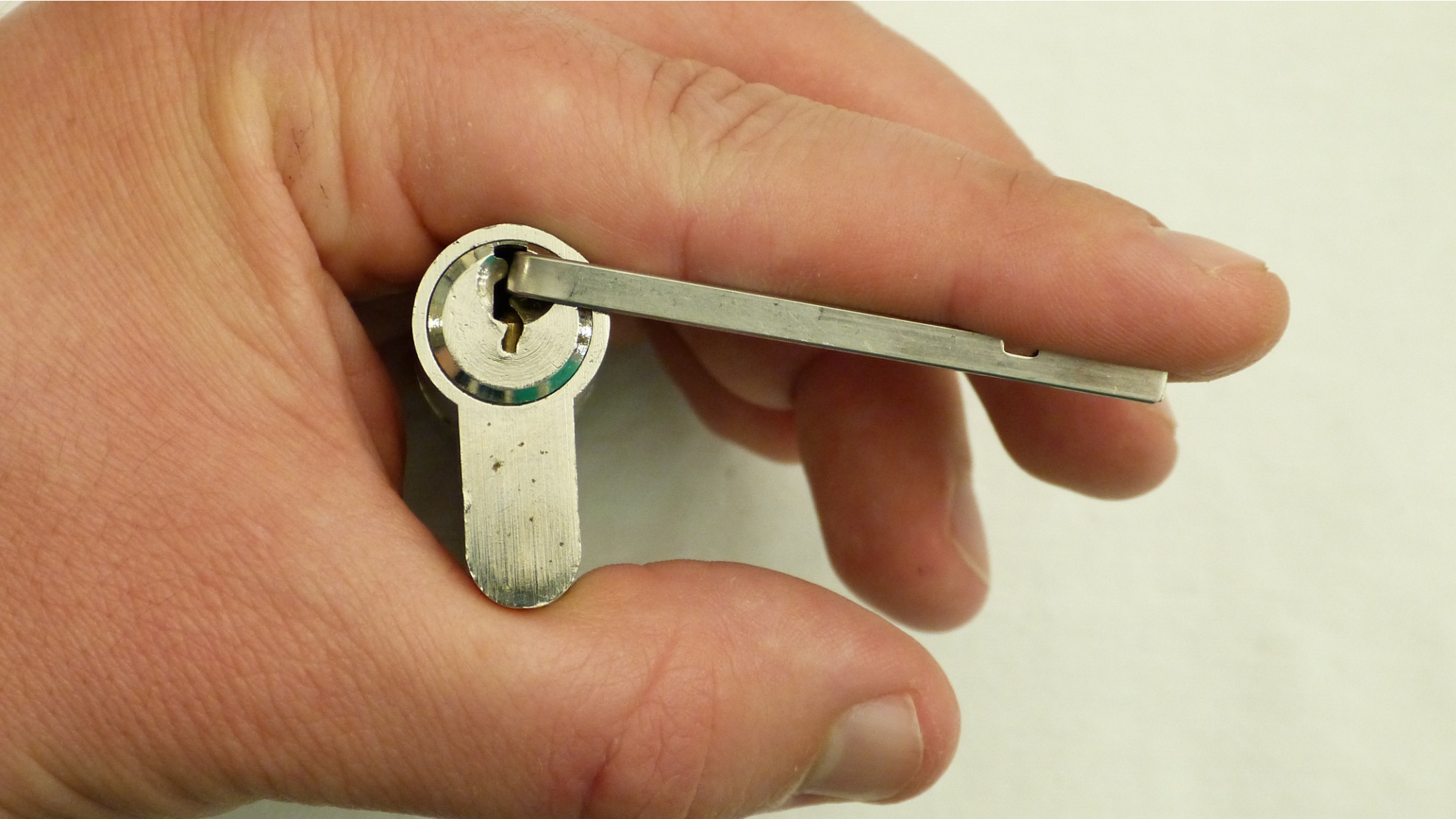


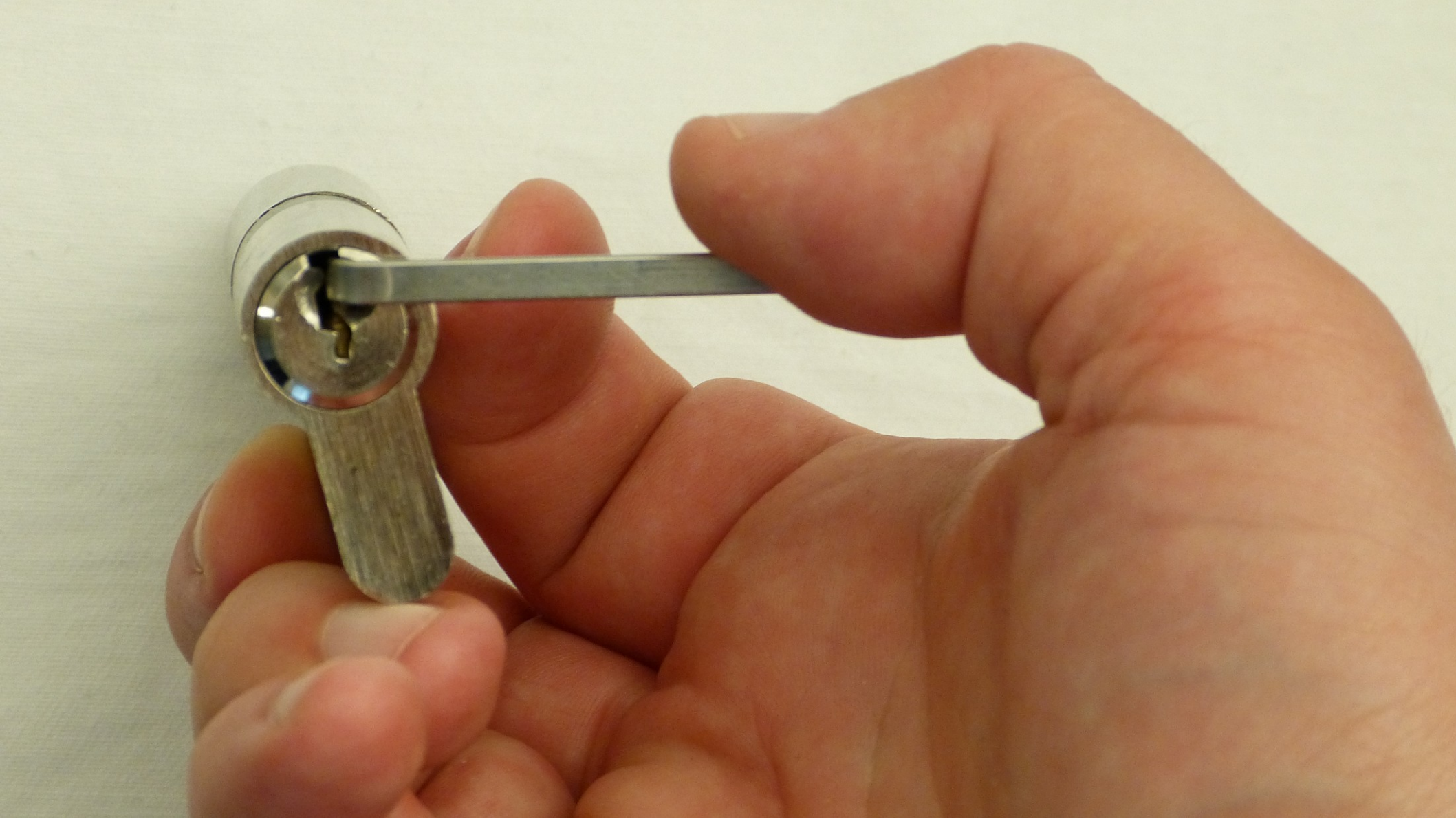






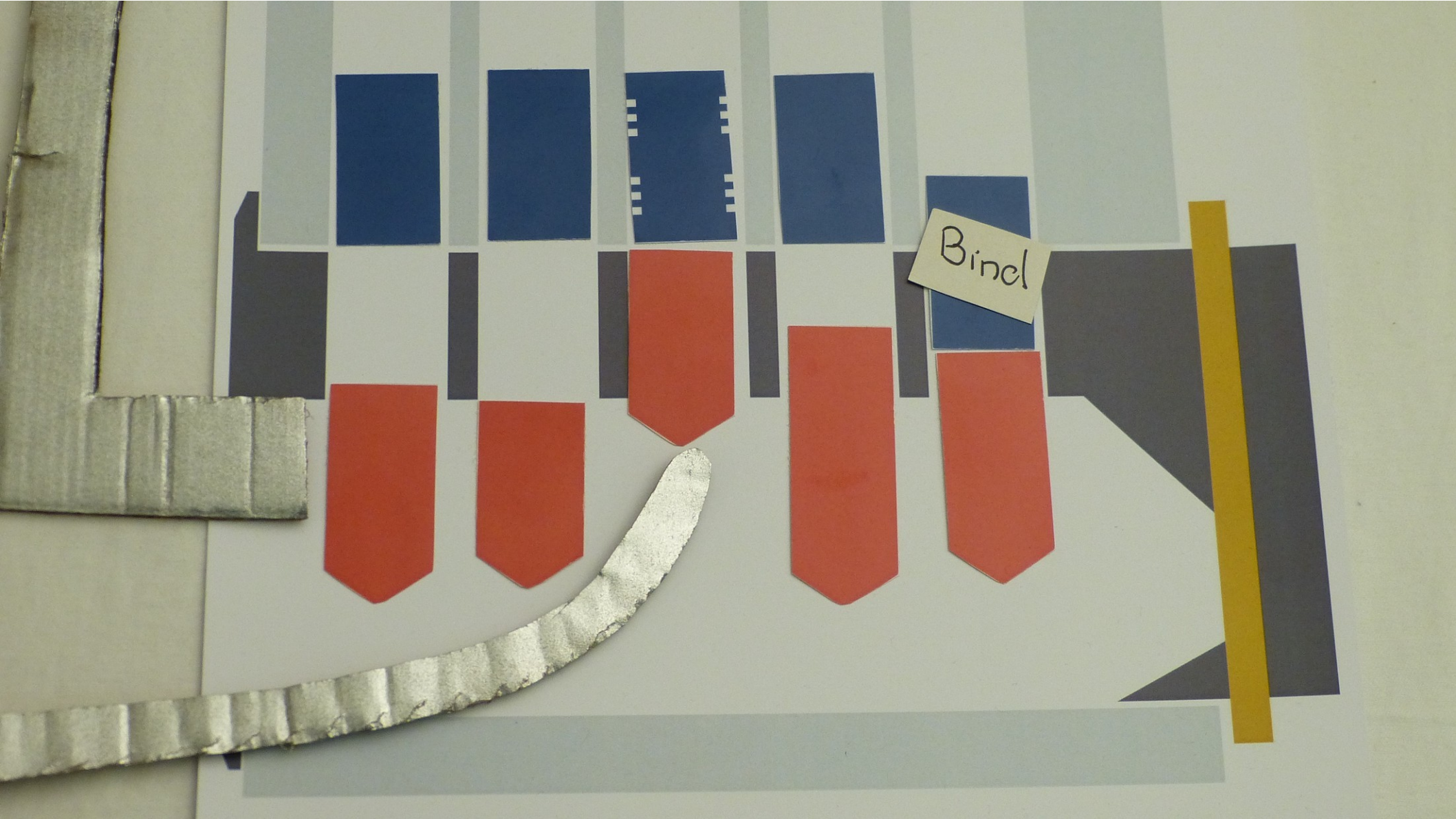


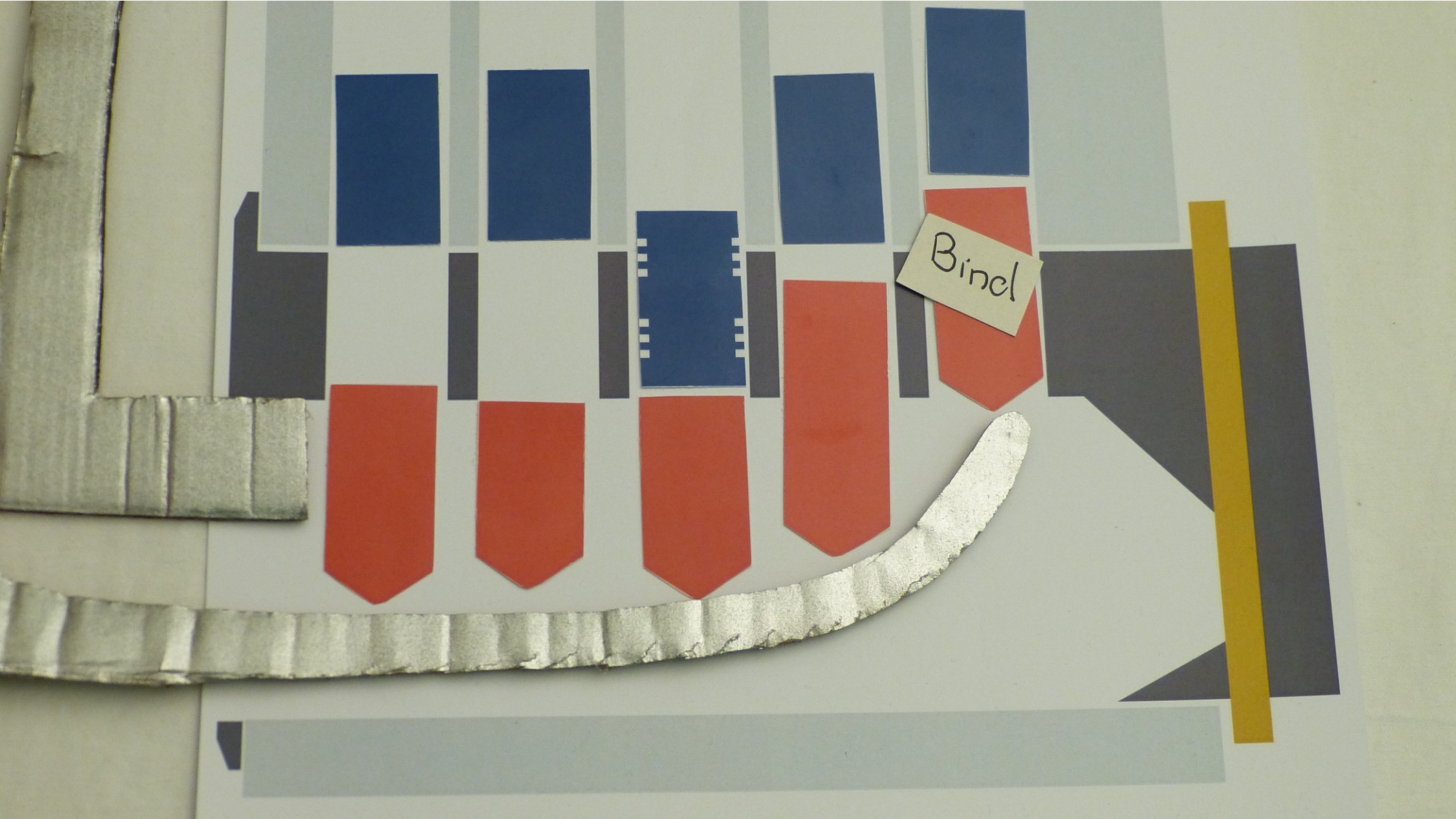




Other pin states

- Non binding
- Binding driver pin
- lose key pin
- Driver pin at shearline
- Overset


Binel

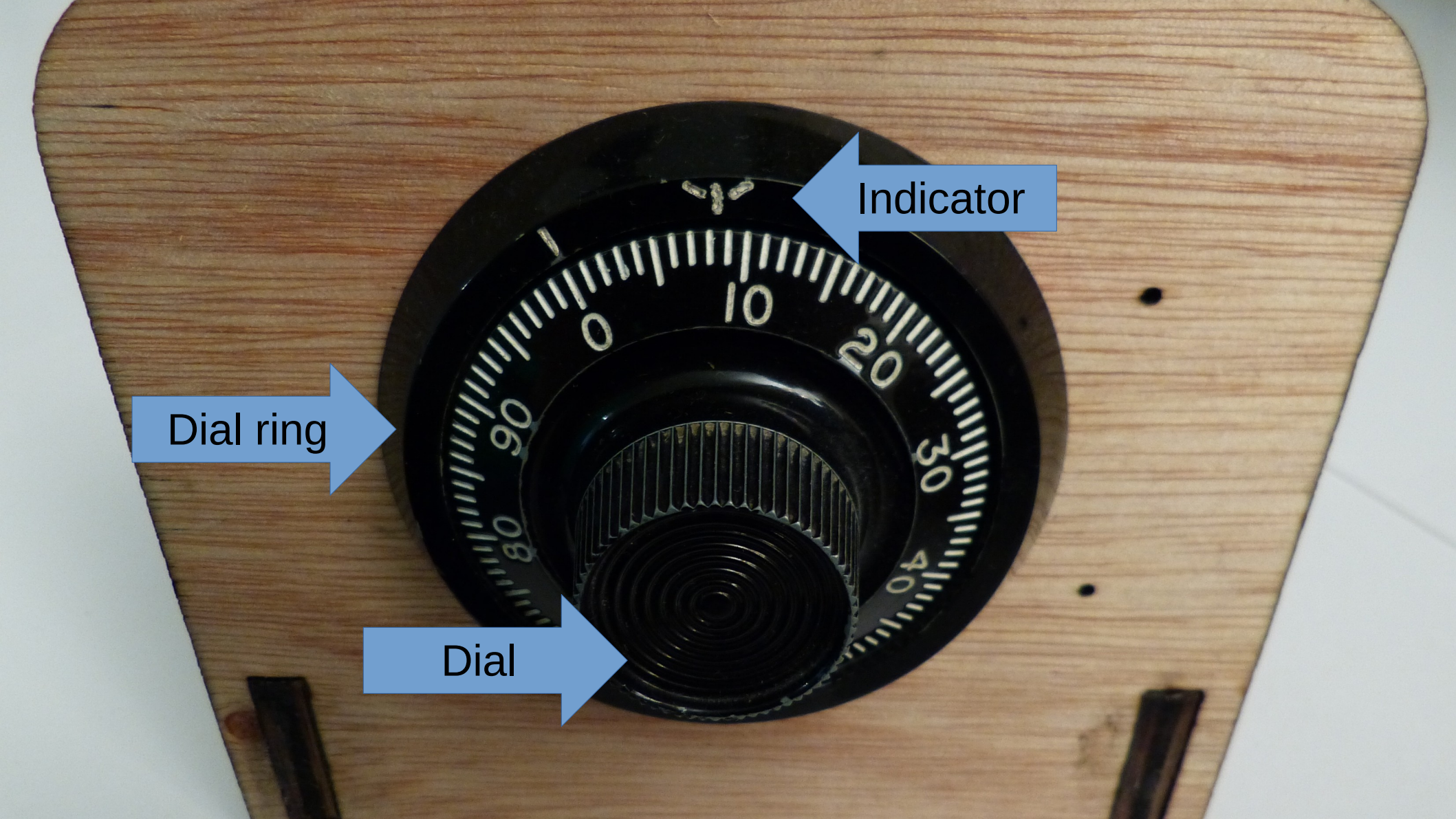

Bindl

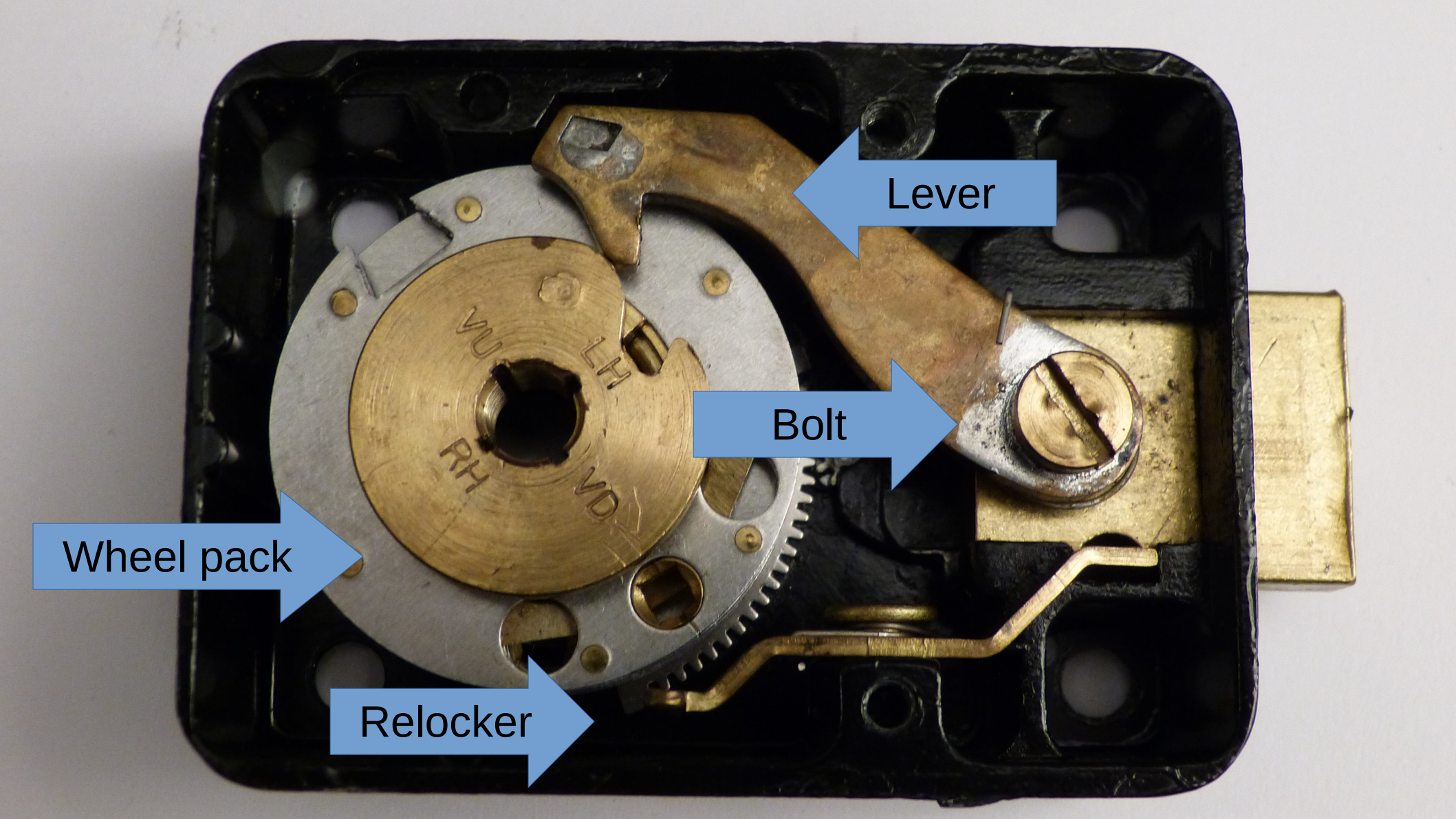
Mechanical Safe Lock

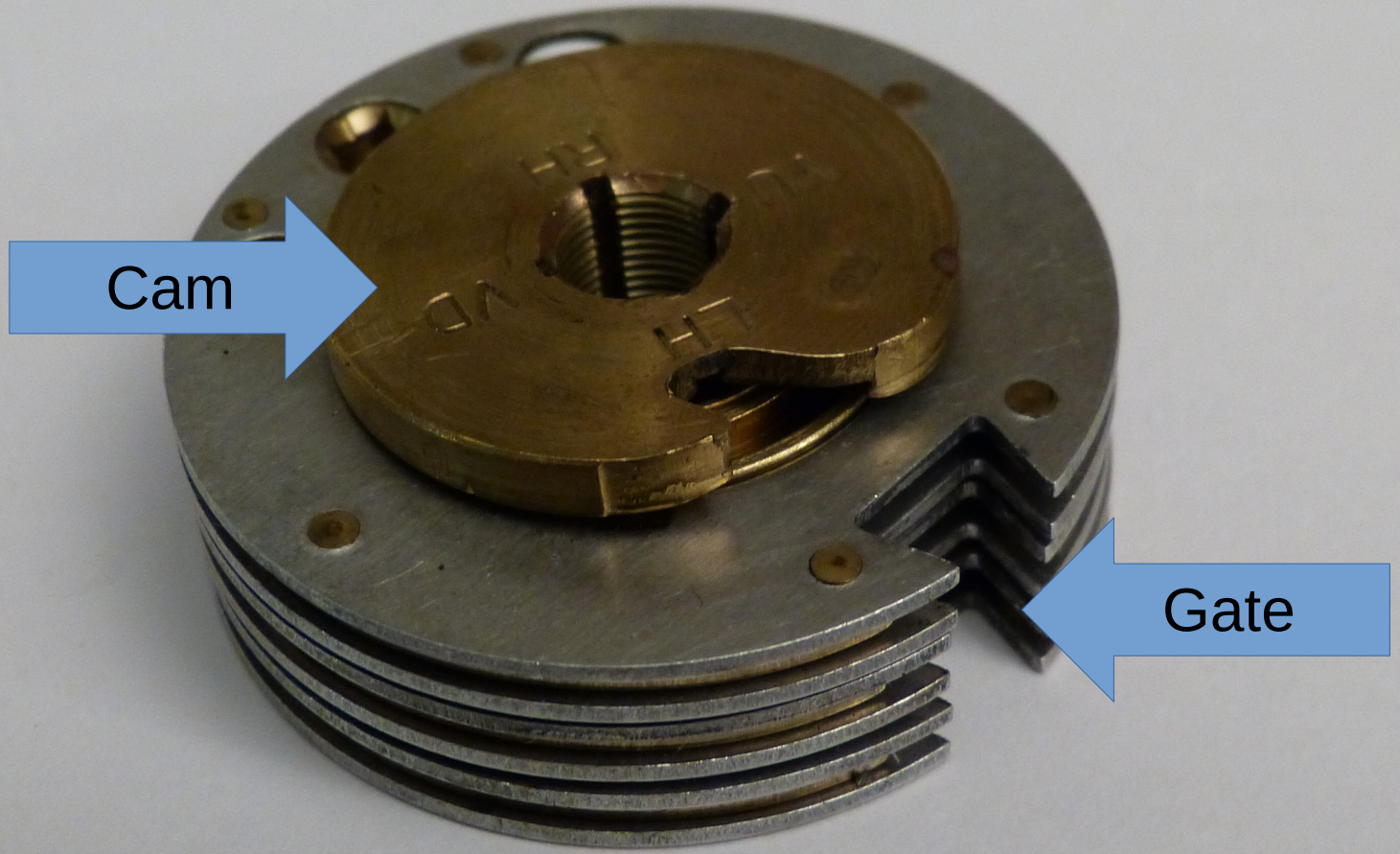
- Spring lever combination lock
  - **Group 2**
    - 2h manipulation resistant
  - **Group 1**
    - Effectively manipulation resistant
  - **Group 1R**
    - X-ray resistant

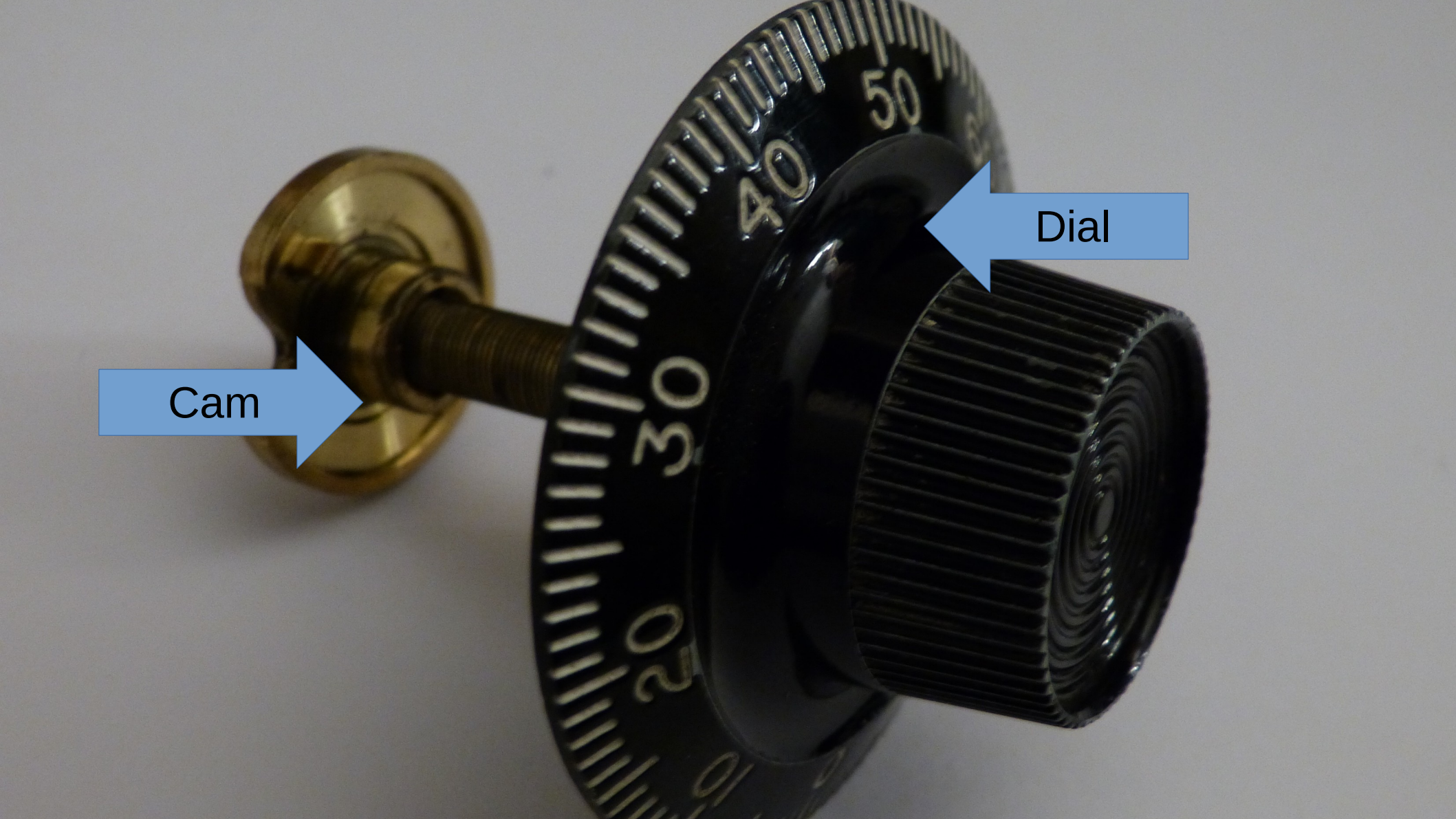
Mechanical Safe Lock

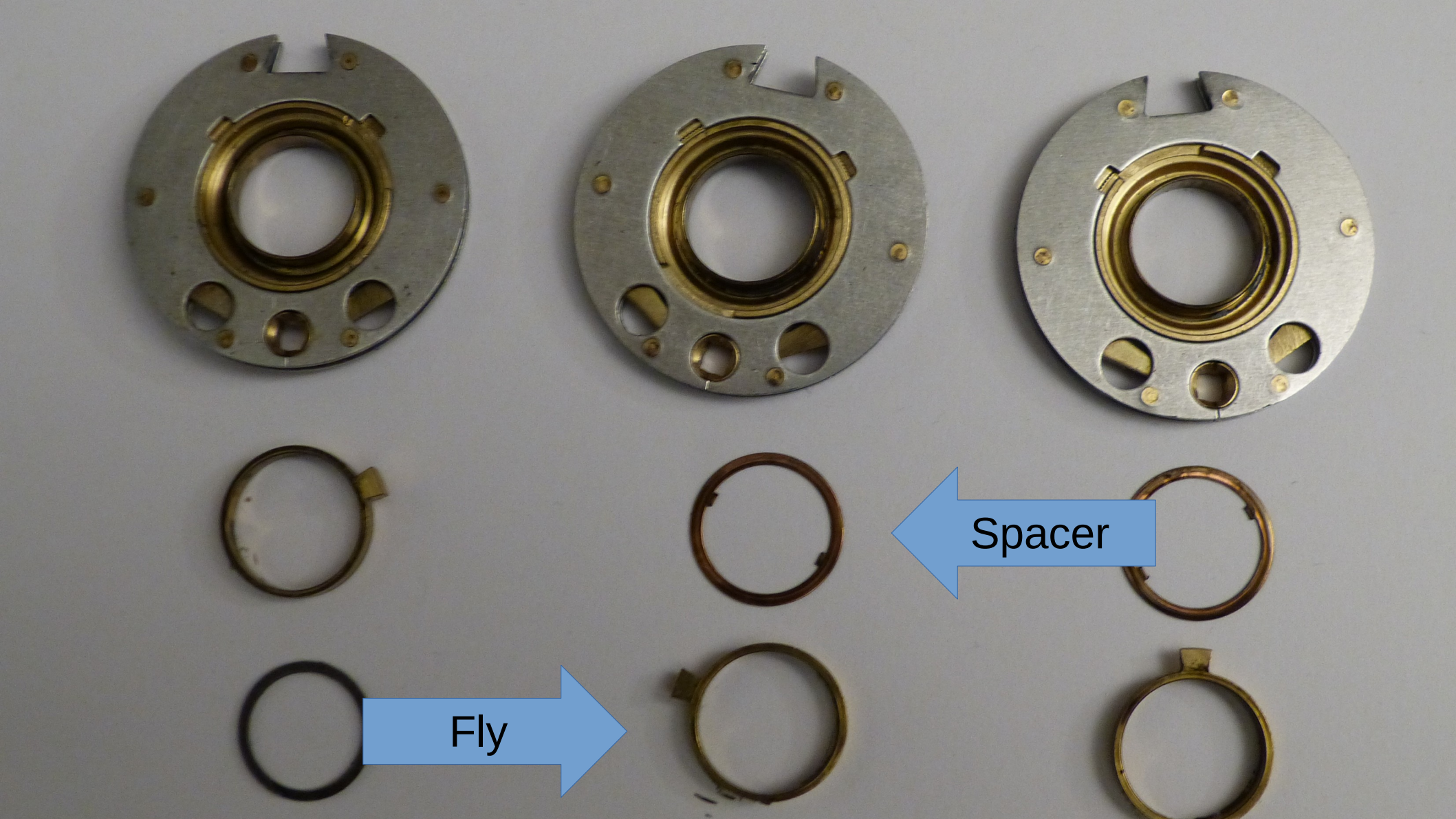
- Target for today:
  - **Sargent Greenleaf 6730**
  - Group 2 safe lock
  - Three wheels
    - Theoretically a million combinations
    - Practically ~400k combinations

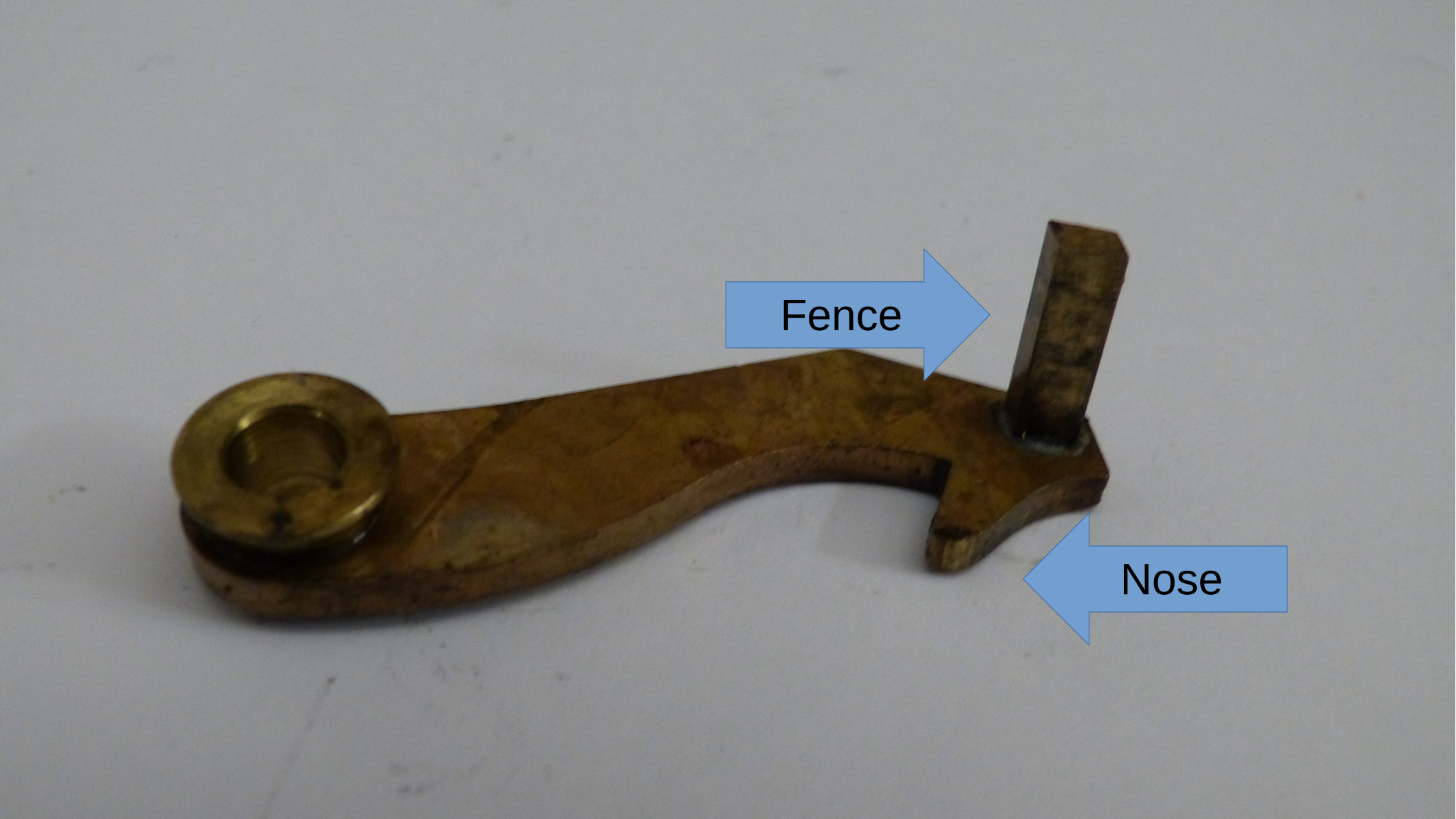

Indicator
Dial ring
Dial
90
80
0
10
20
30
40


Lever
Bolt
Wheel pack
Relocker
VU
LH
RH
VD


Cam
Gate


Cam
Dial
50
40
30
20


Spacer
Fly


Fence
Nose

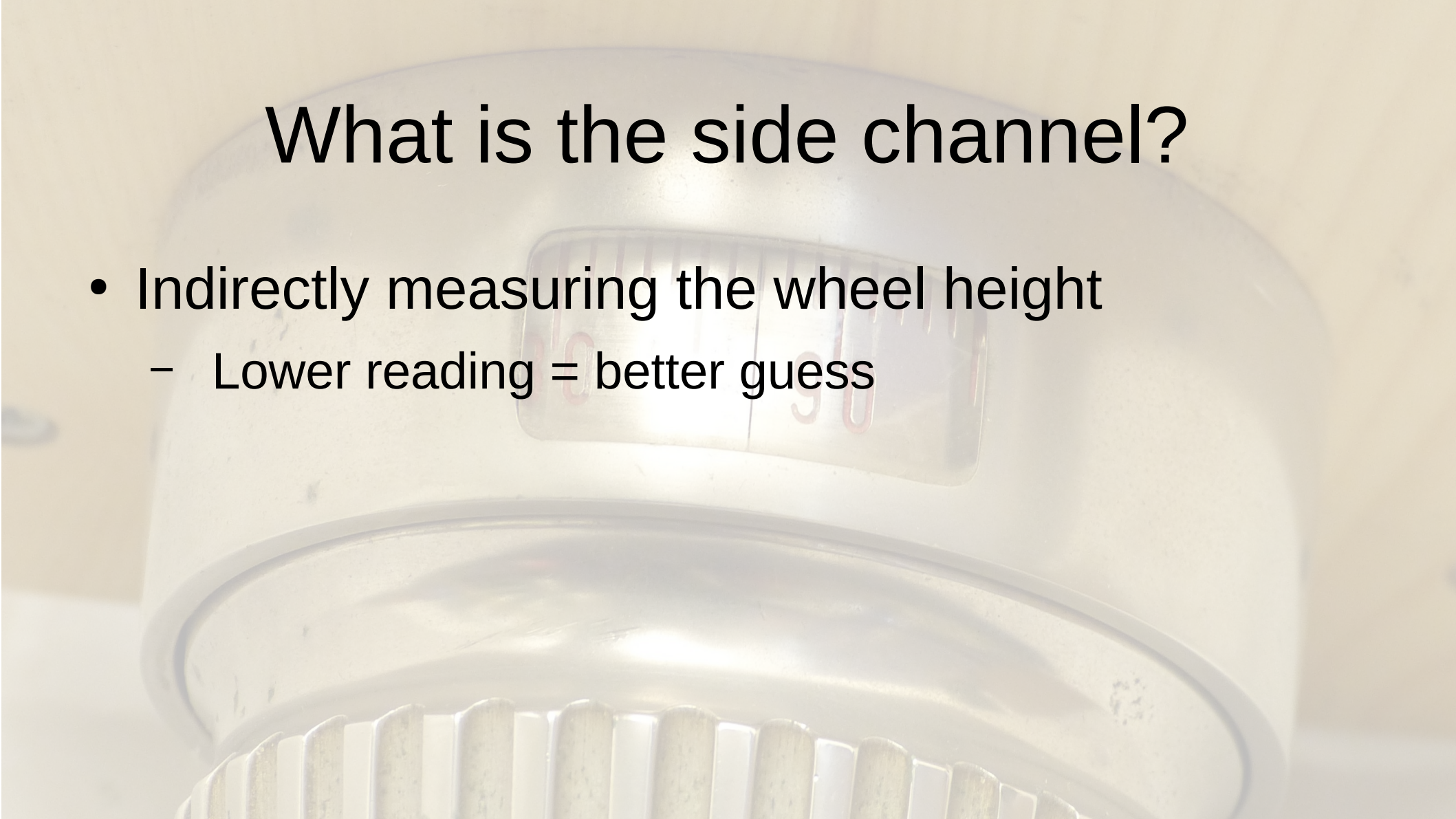

LH
VU
VD
RH

Dialing sequence

- Left **four times** to the **first** number
- Right **three times** to the **second** number
- Left **twice** to the **last** number
- Right **past zero** to open the lock

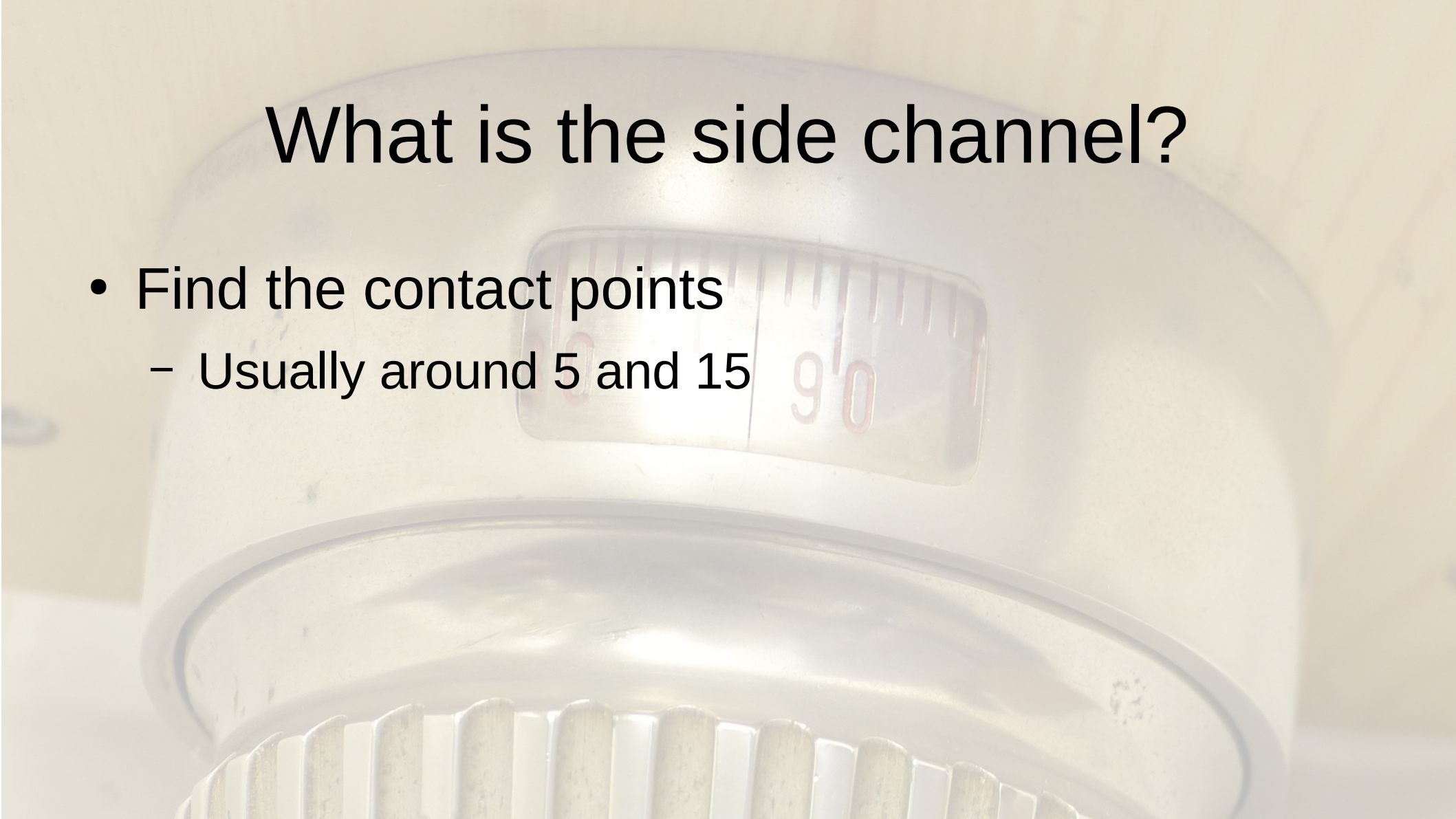
What is the side channel?

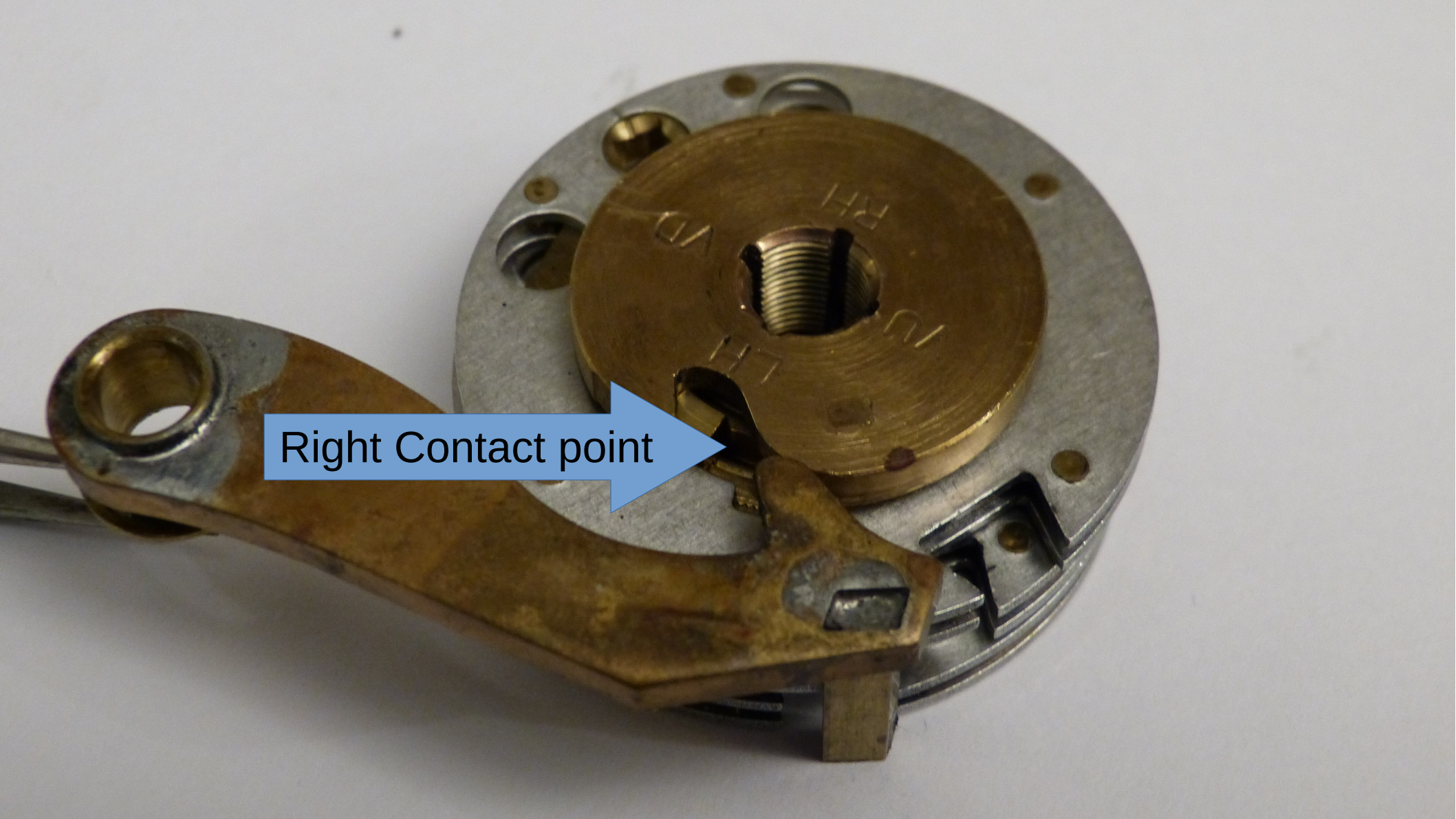
- Indirectly measuring the wheel height
  - Lower reading = better guess

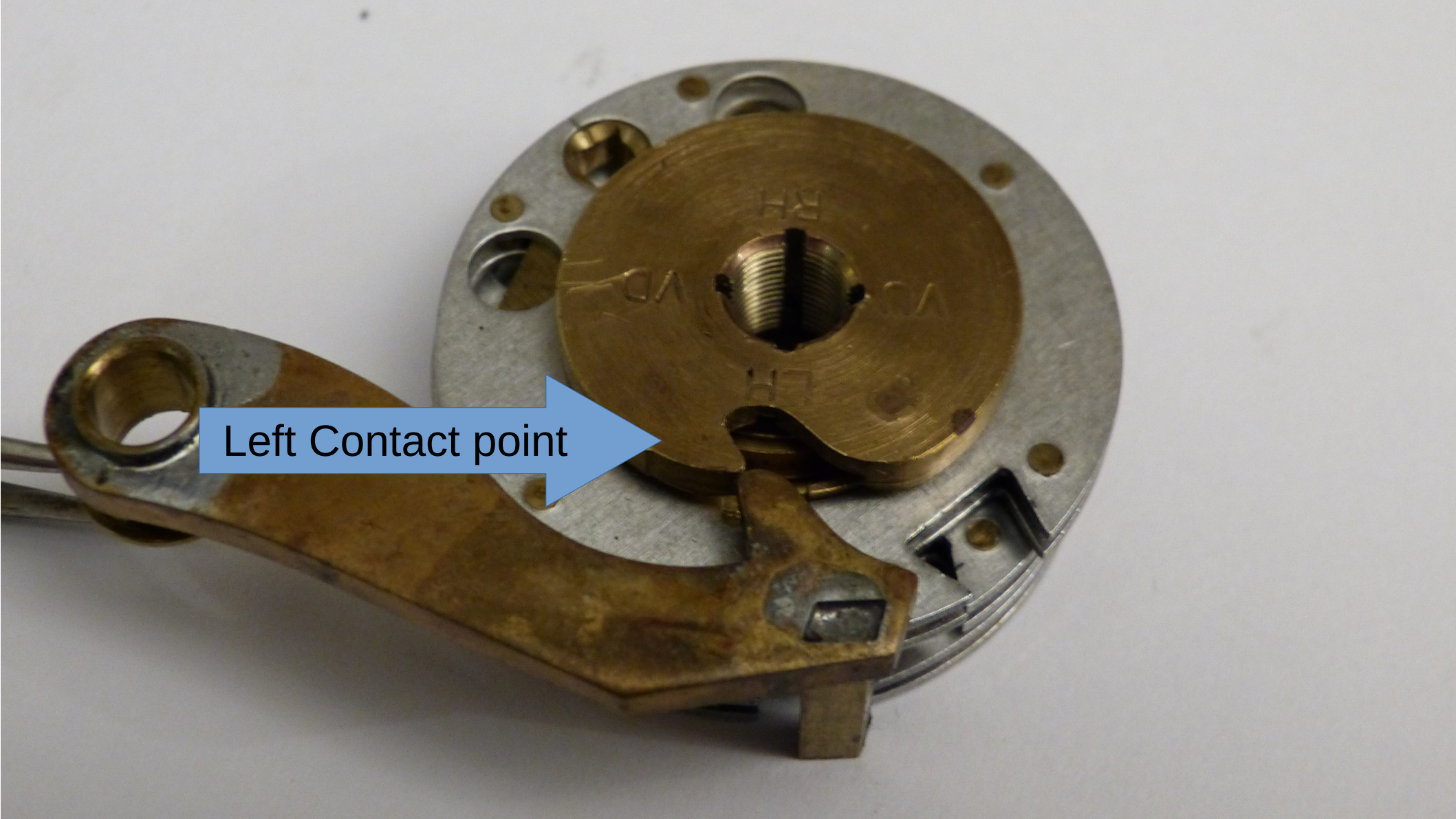


What is the side channel?

- Find the contact points
  - Usually around 5 and 15




Right Contact point

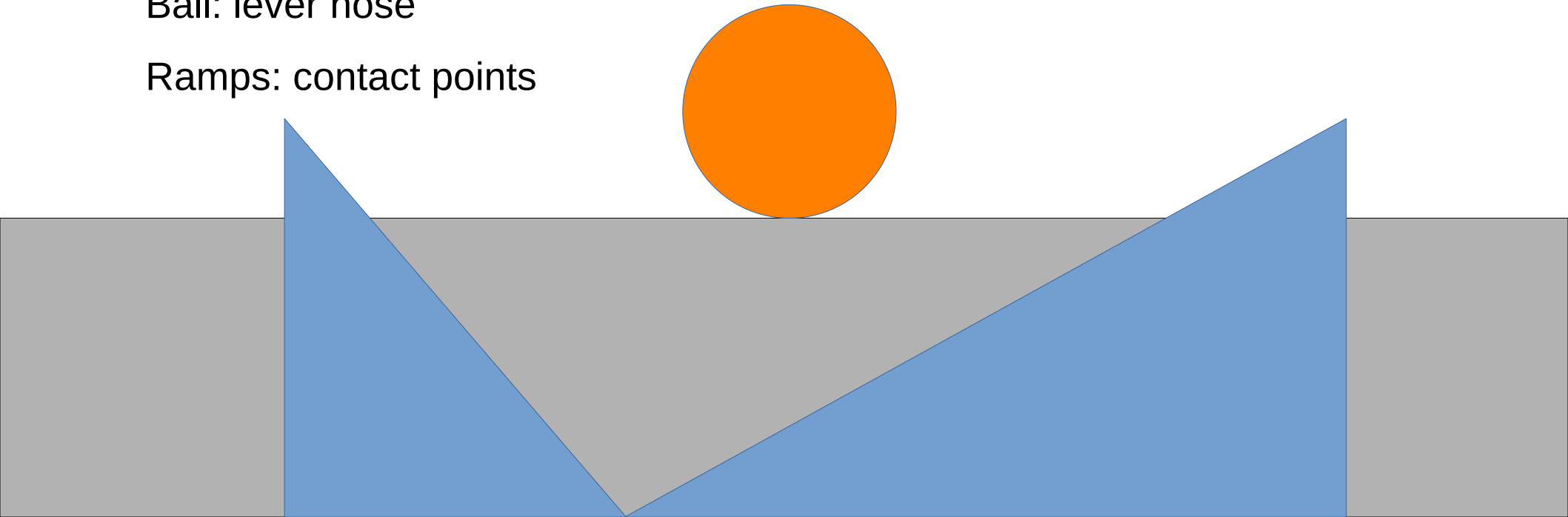

RH
LH
Left Contact point

Manipulation process

Gray: Wheel

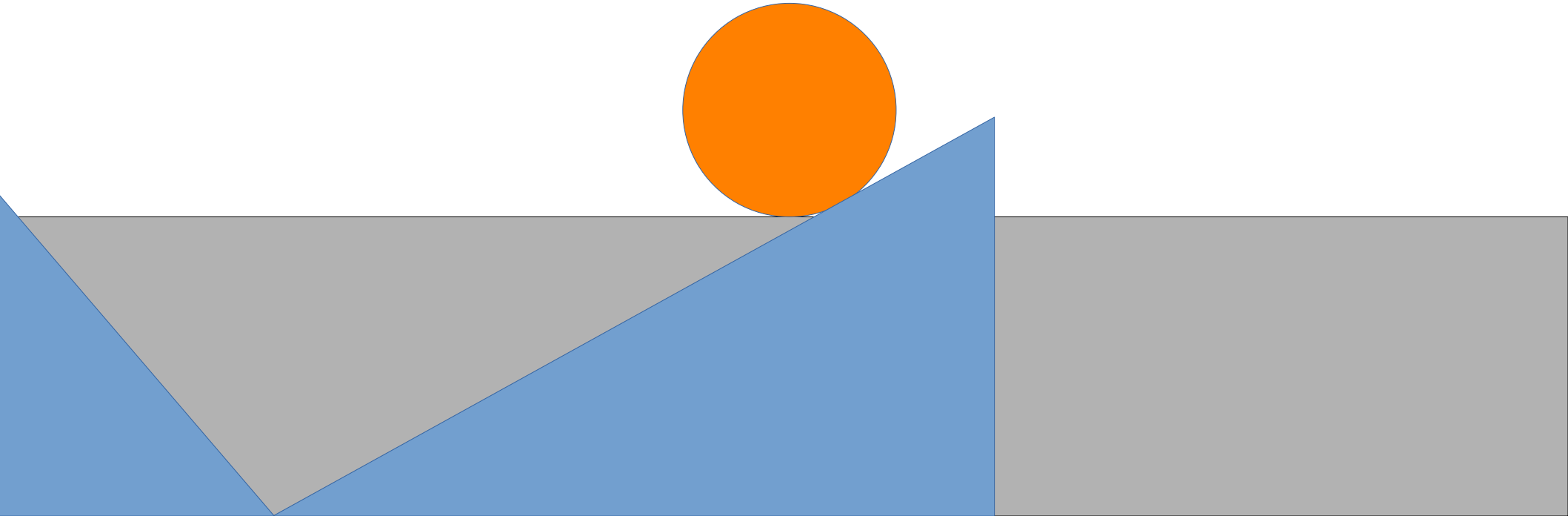
Ball: lever nose

Ramps: contact points



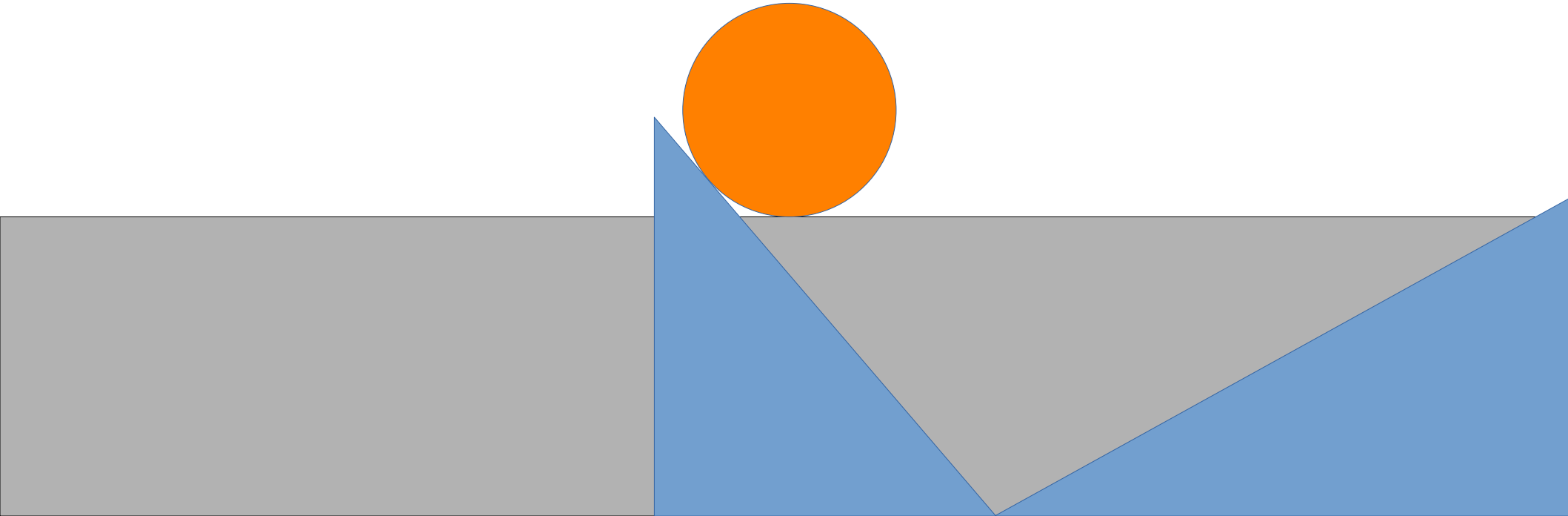
Manipulation process

Right contact point

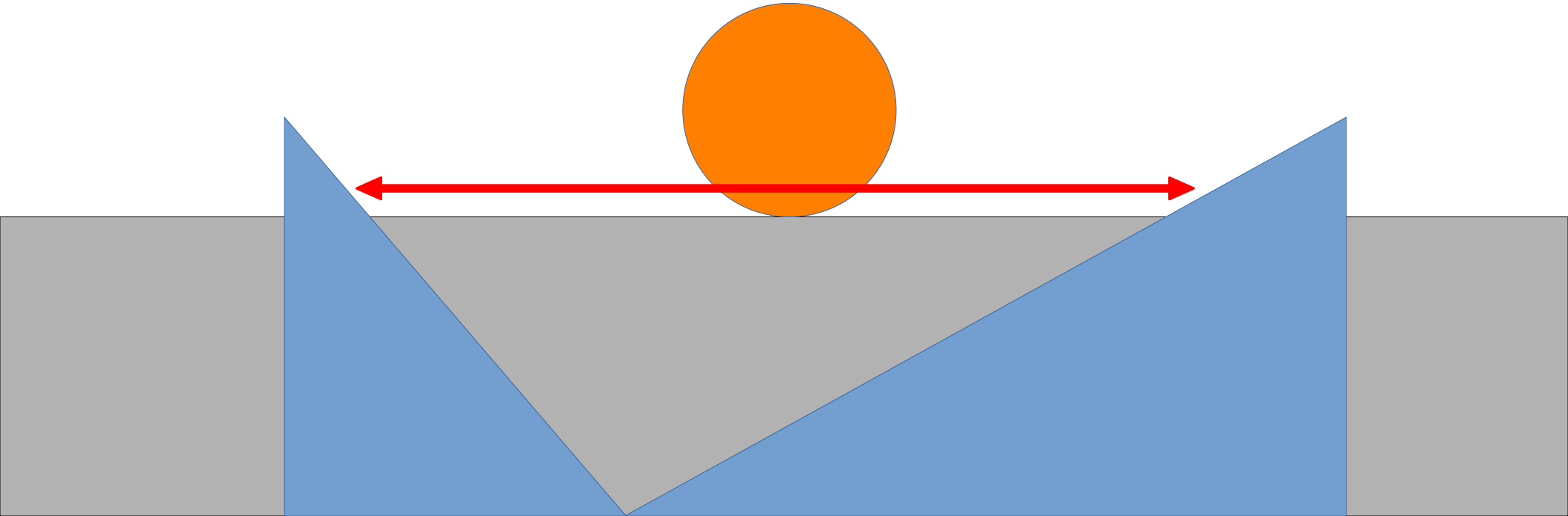


Manipulation process

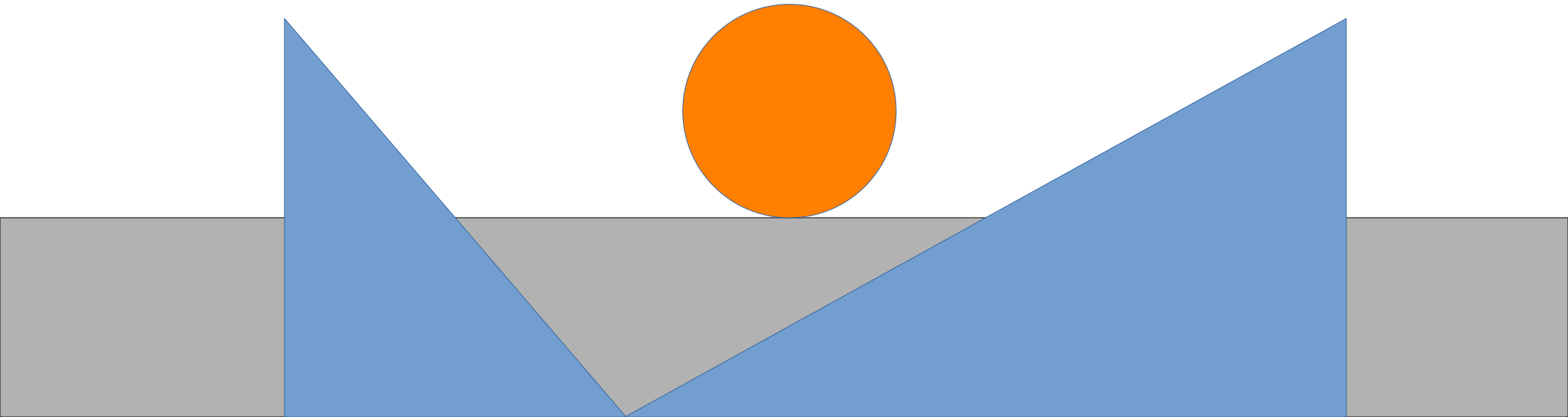
Left contact point



Manipulation process

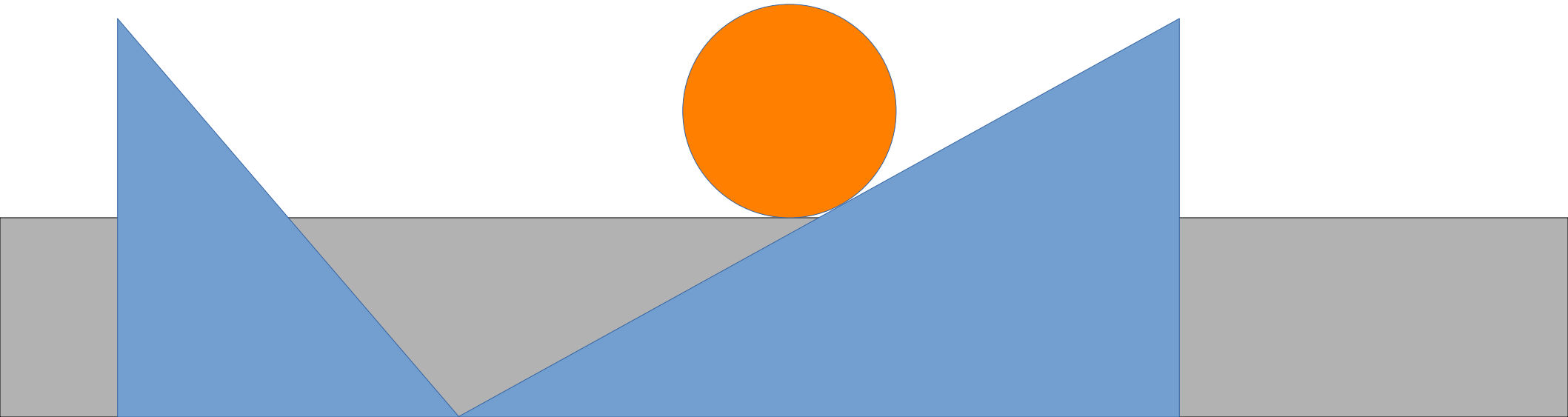


Manipulation process



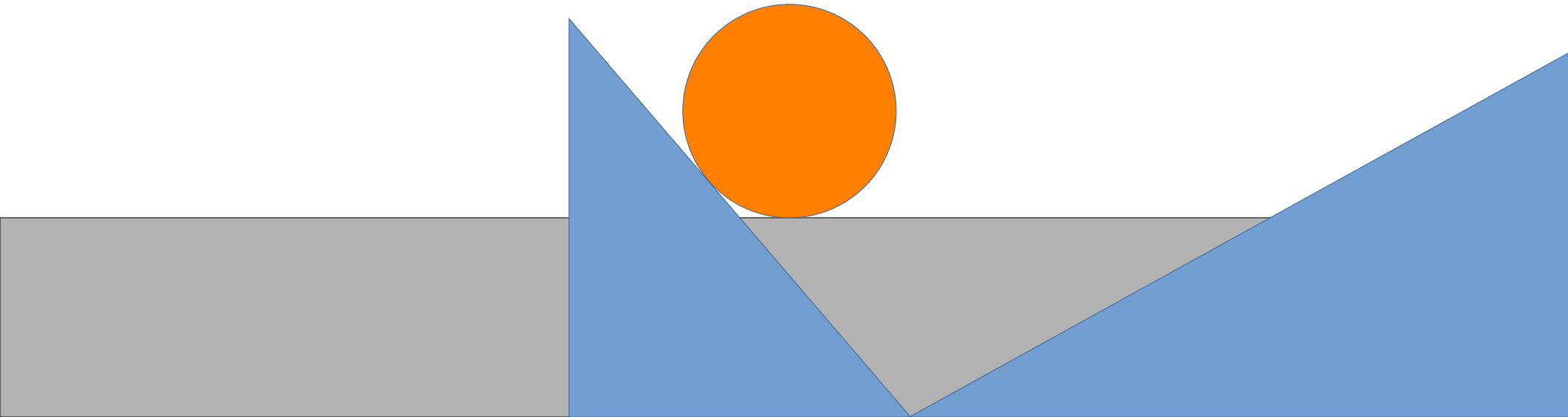
Manipulation process

Right contact point

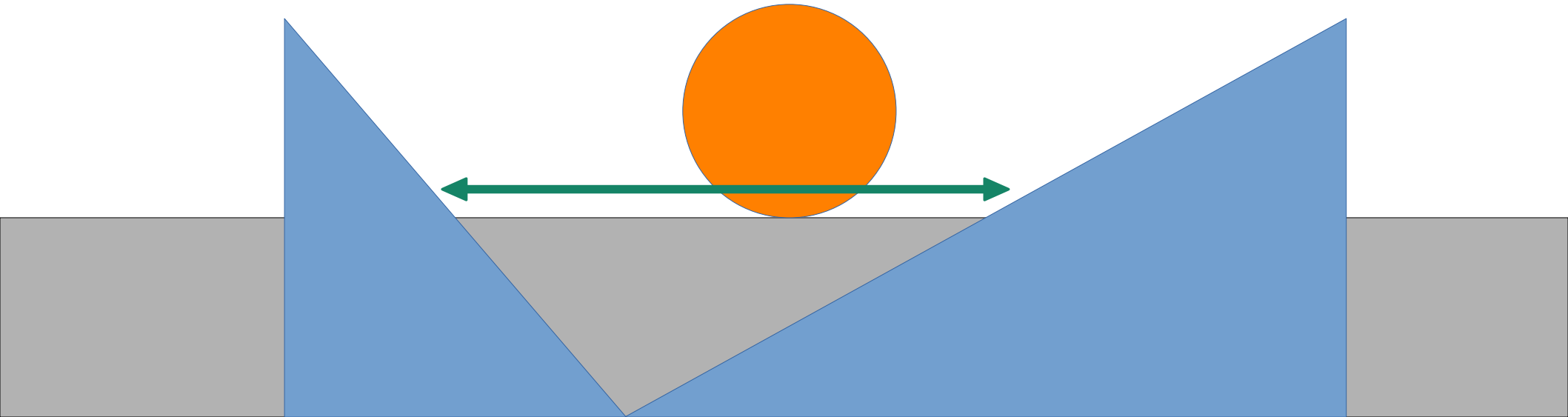


Manipulation process

Left contact point

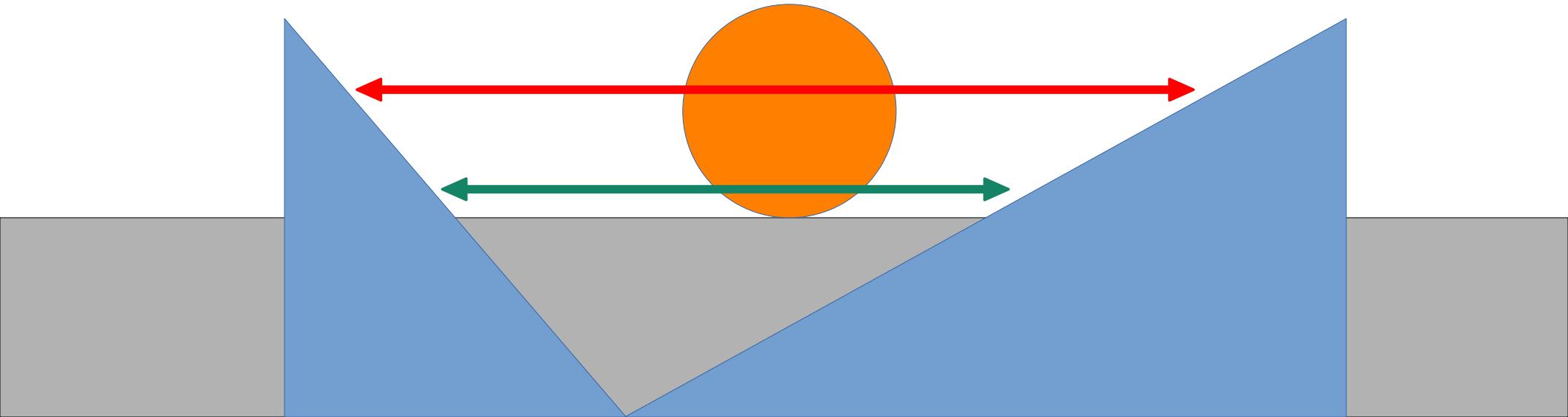


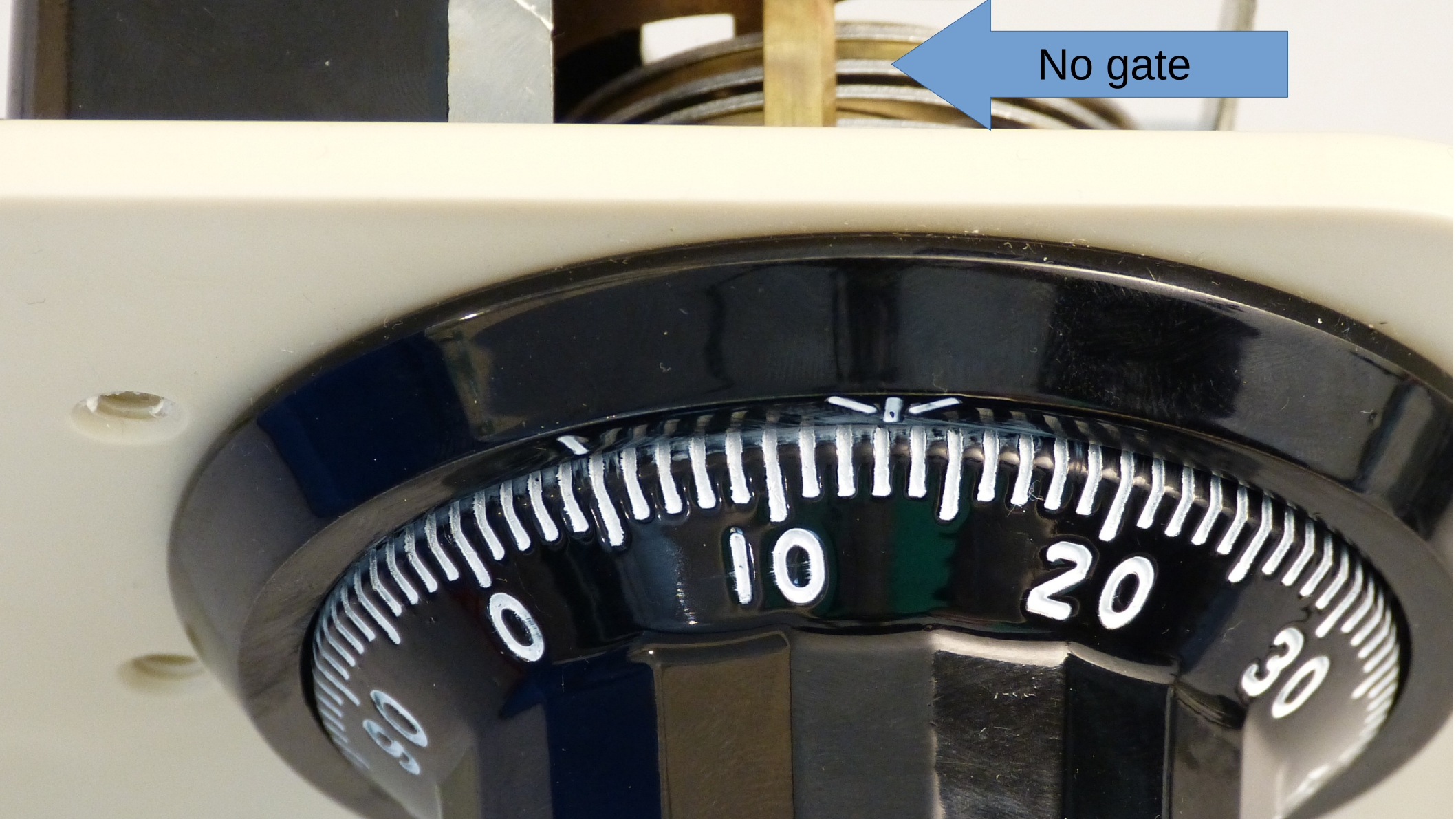
Manipulation process

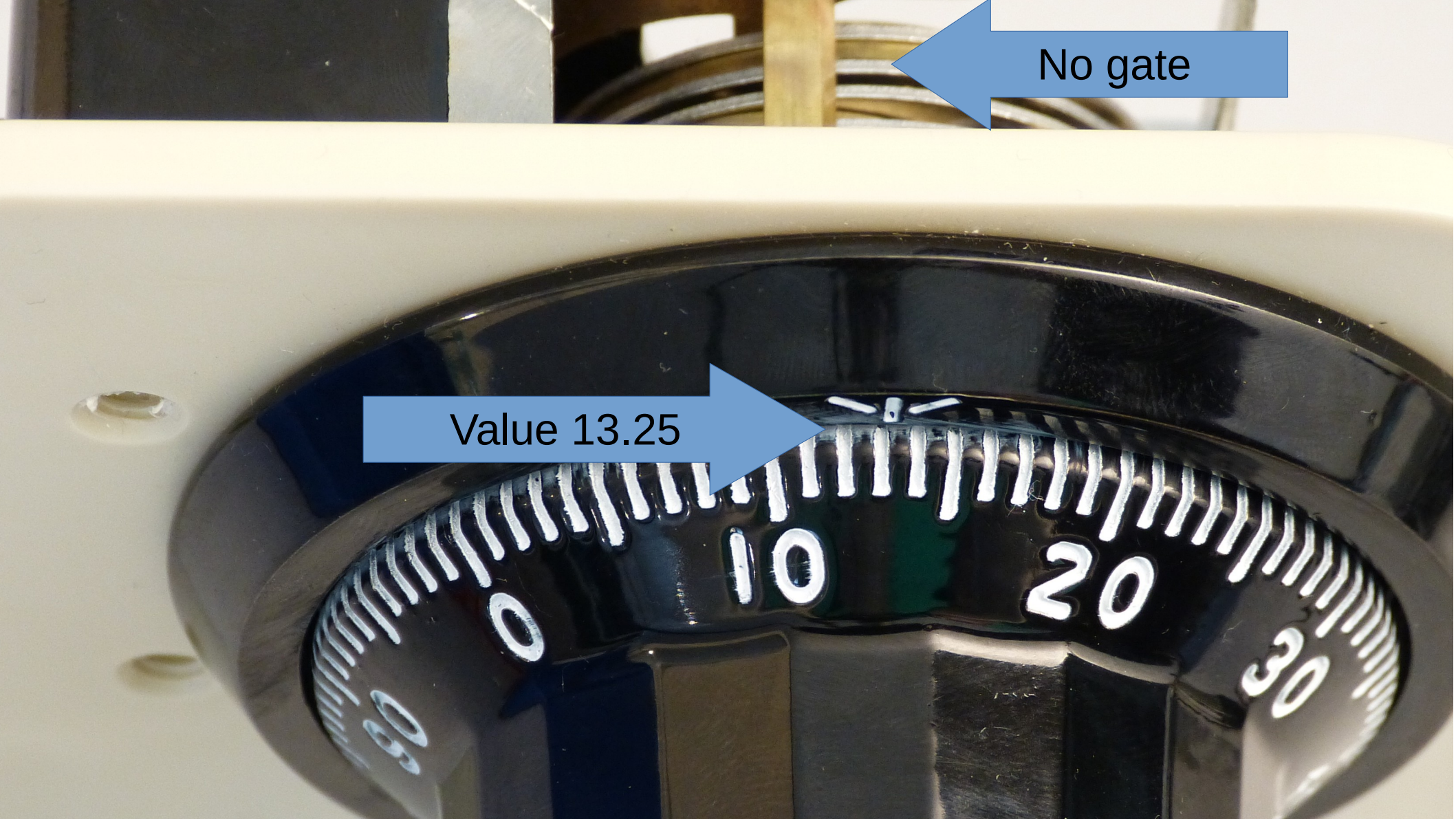


Manipulation process

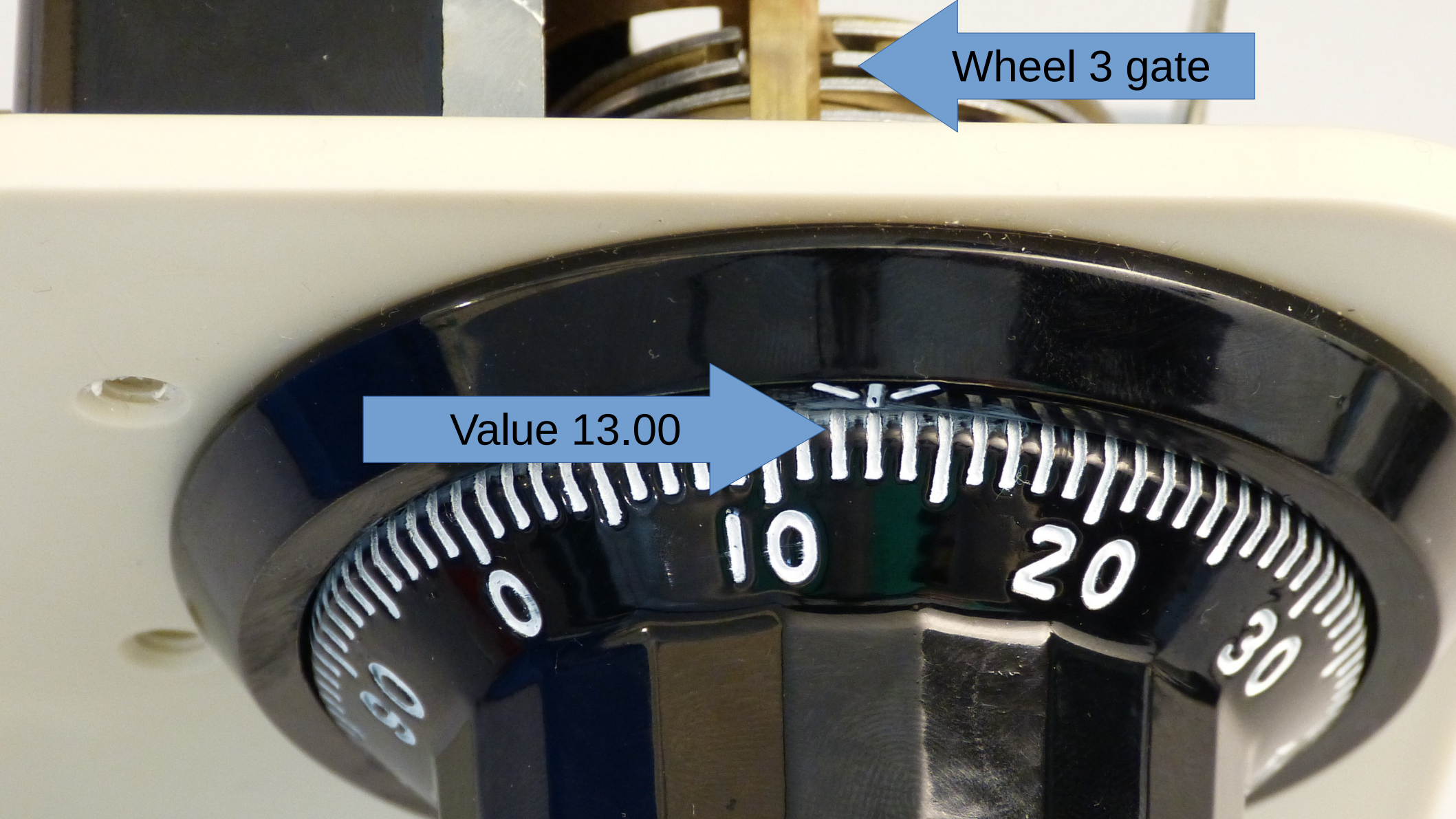
Shorter distance = more correct




No gate
0
10
20
30


No gate
Value 13.25
0
10
20
30


Gate of wheel 3
0
10
20
30

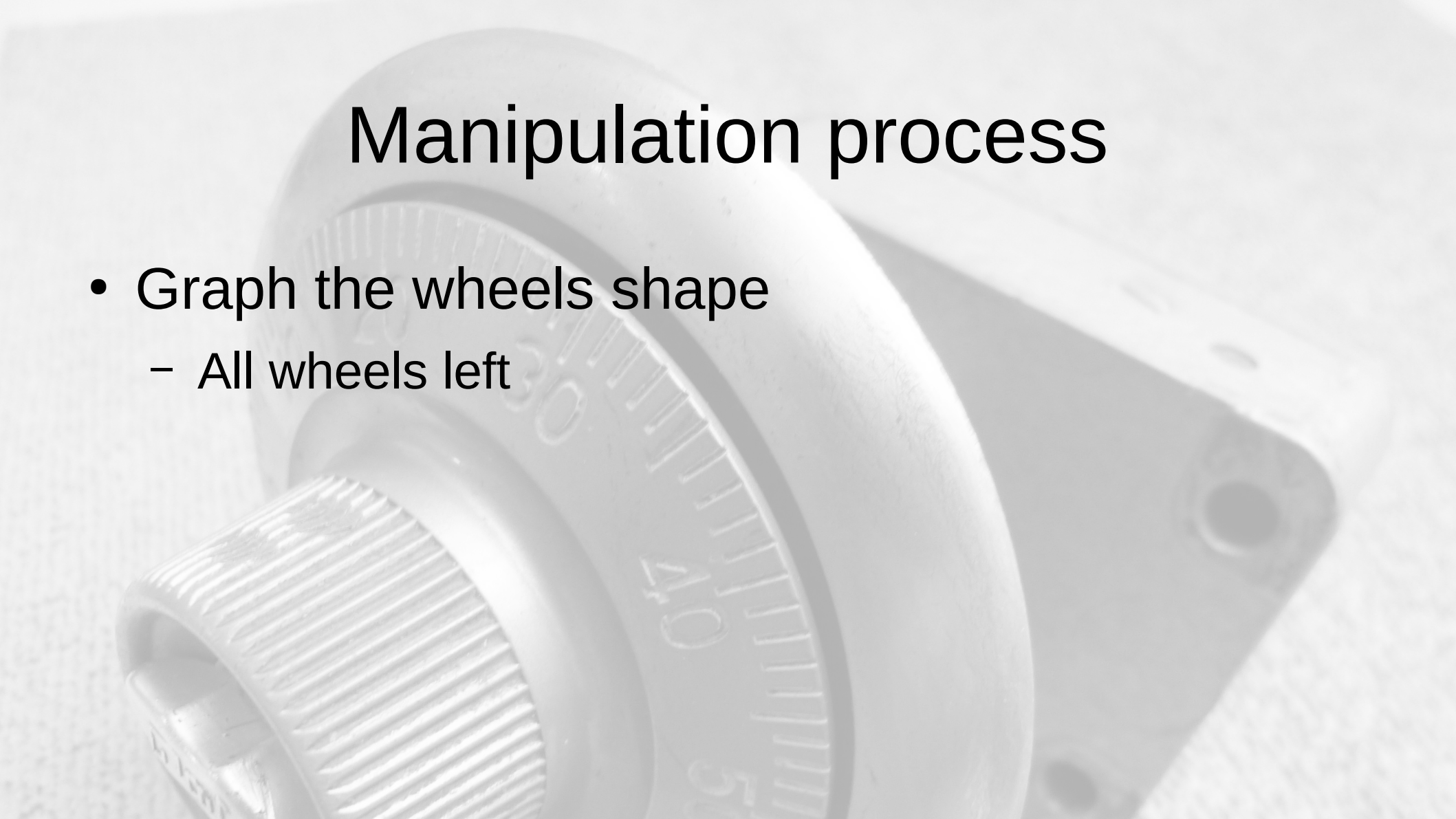

Wheel 3 gate
Value 13.00
0
10
20
30

Manipulation process

- Measuring precision
  - Traditionally 1/8th of a digit
  - 0.1 increments work as well

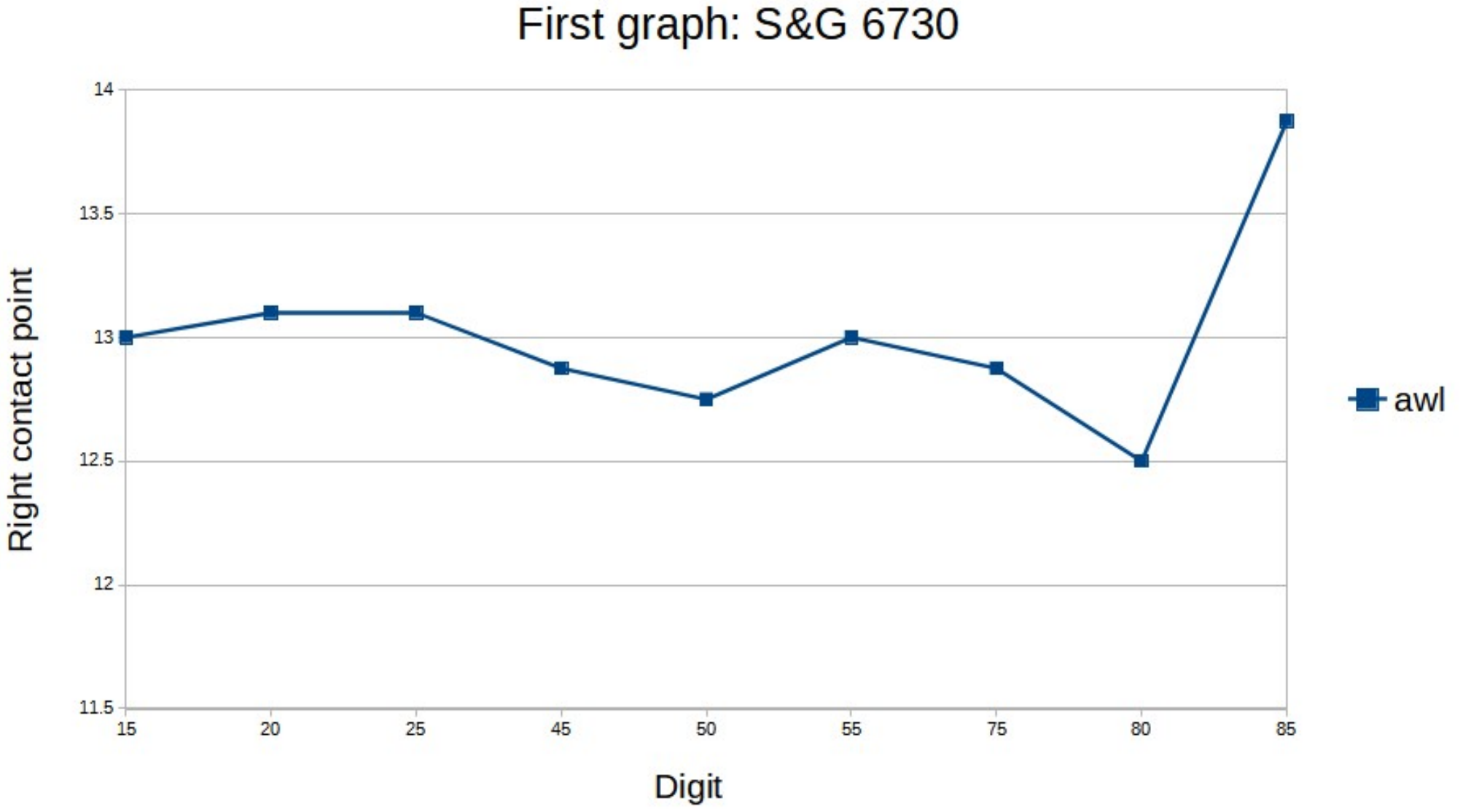
Manipulation process

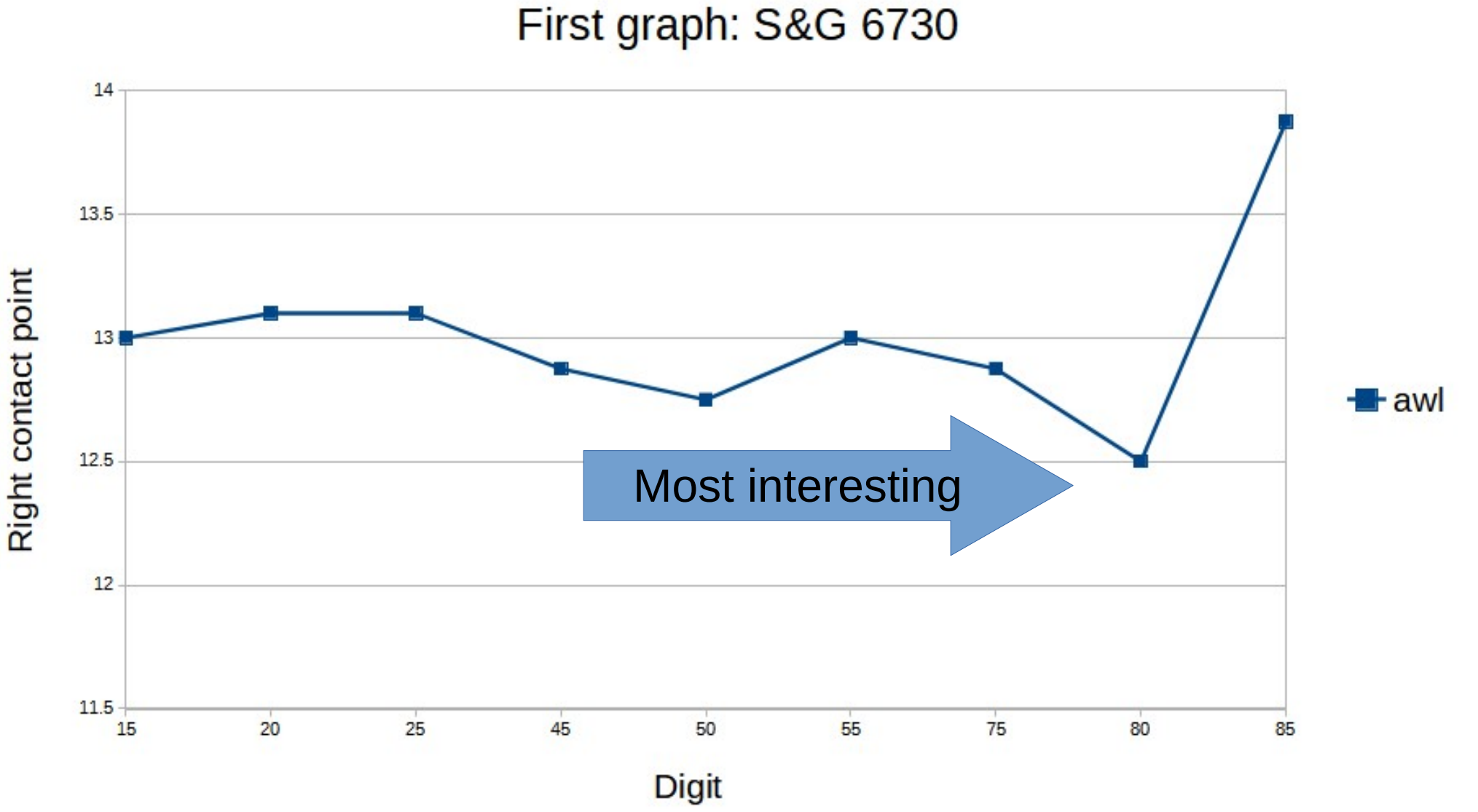
- Graph the wheels shape
  - All wheels left



Manipulation process

- All wheels left:
  1) Dial four times left and stop at n
  2) Dial back to measure contact point
  3) Dial left to n + 2.5
  4) Completed the graph?
     1) Yes: Finished
     2) No: Go to 2


First graph: S&G 6730
Right contact point
14
13.5
13
12.5
12
11.5
15
20
25
45
50
55
75
80
85
Digit
awl


First graph: S&G 6730
Right contact point
14
13.5
13
12.5
12
11.5
15
20
25
45
50
55
75
80
85
Digit
awl
Most interesting

Manipulation process

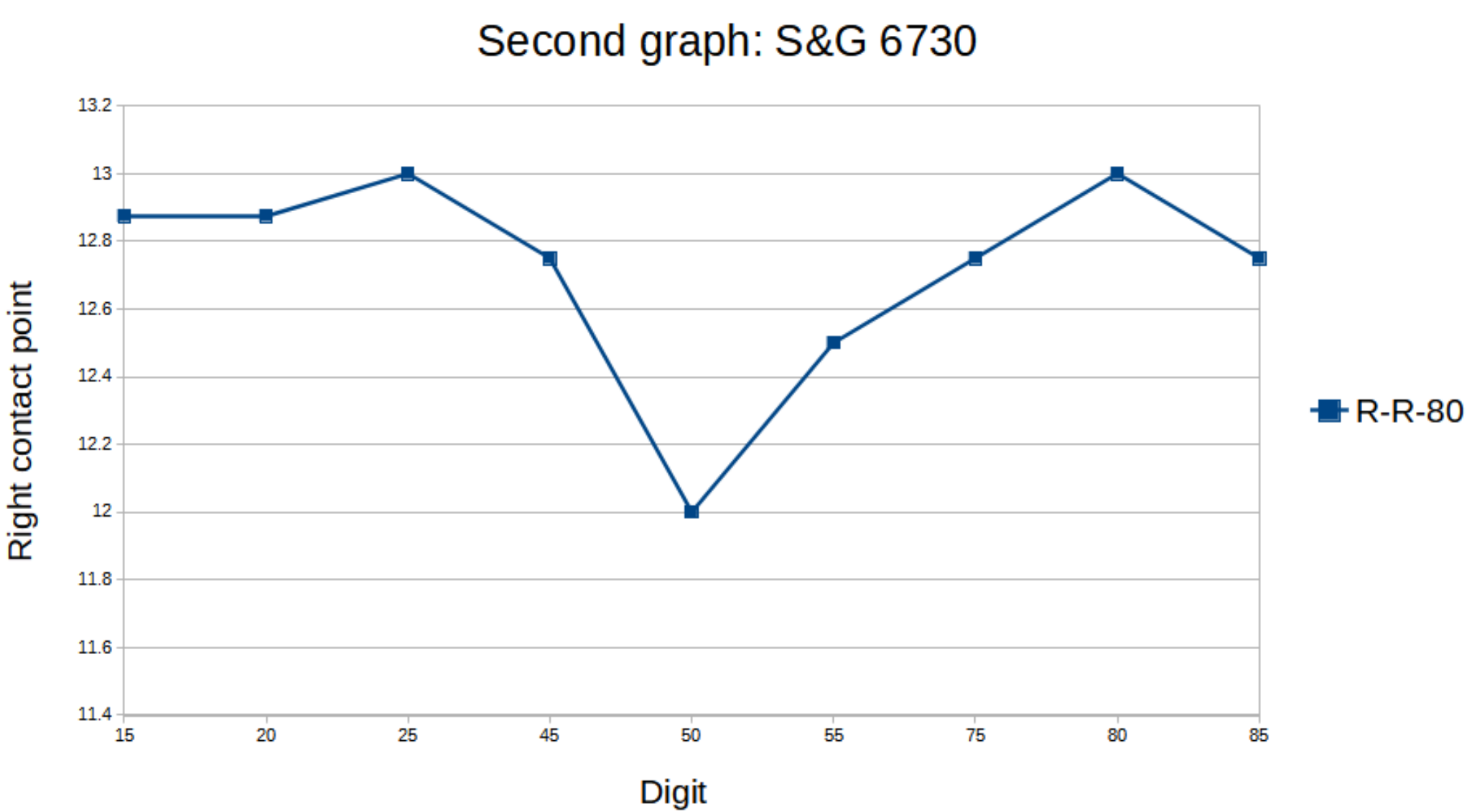
- We need to test which wheel is the lowest point is
  - We dial:
    - 80L 80L 70R and take a reading
    - 70R 80L 80L and take a reading
    - 80L 70R 80L and take a reading

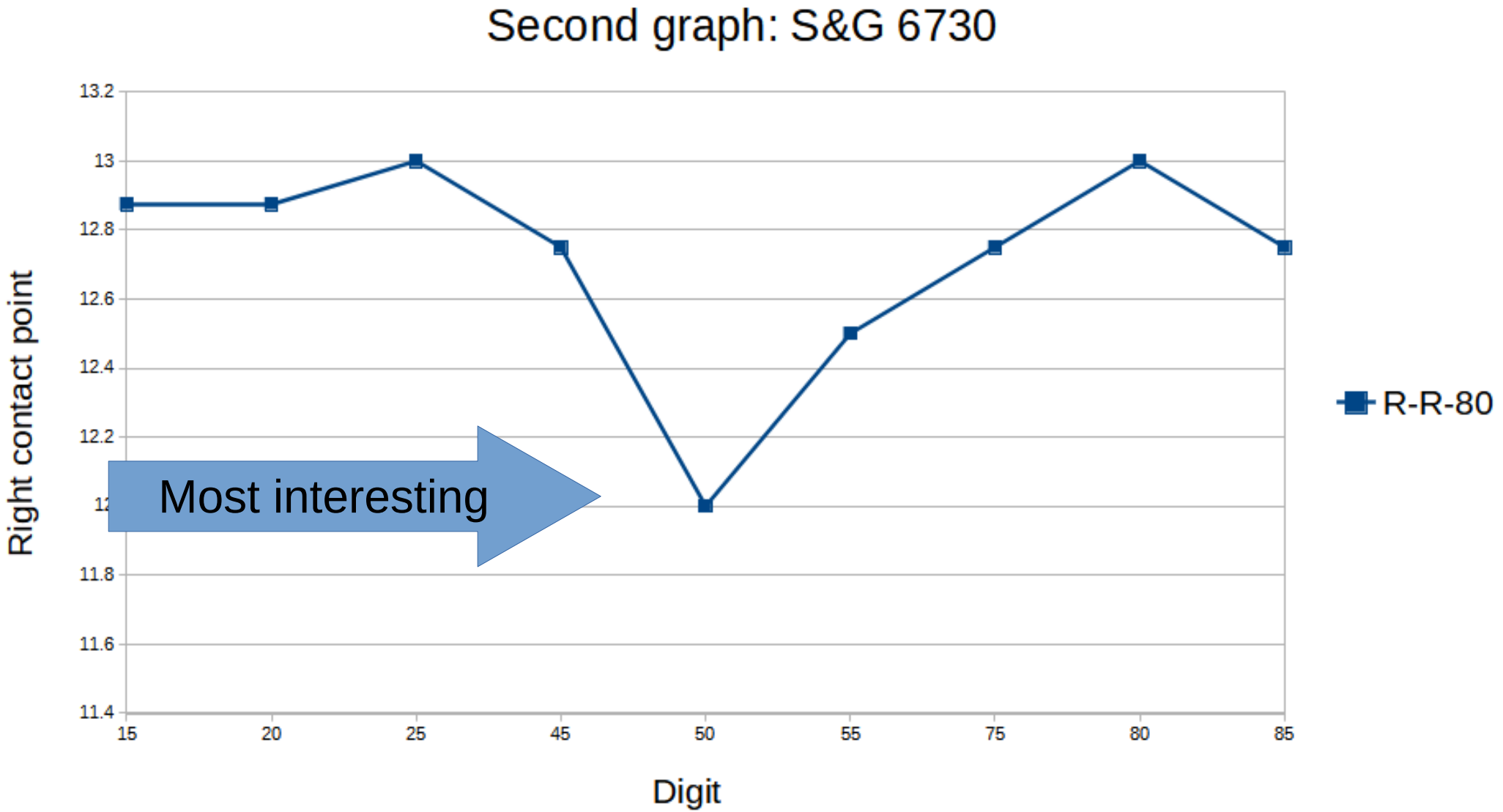
Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 80L 80L 70R 13
    - 70R 80L 80L 12.5
    - 80L 70R 80L 12.5

Manipulation process

- With 80 left on the third wheel we make a new graph: Right Right 80L


Second graph: S&G 6730
Right contact point
13.2
13
12.8
12.6
12.4
12.2
12
11.8
11.6
11.4
15
20
25
45
50
55
75
80
85
Digit
R-R-80


Second graph: S&G 6730
Right contact point
13.2
13
12.8
12.6
12.4
12.2
12
11.8
11.6
11.4
15
20
25
45
50
55
75
80
85
Digit
R-R-80
Most interesting

Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 50L 40R 80L 13
    - 40L 50R 80L 12

Manipulation process

- Brute force the last number or make another graph.

Manipulation process

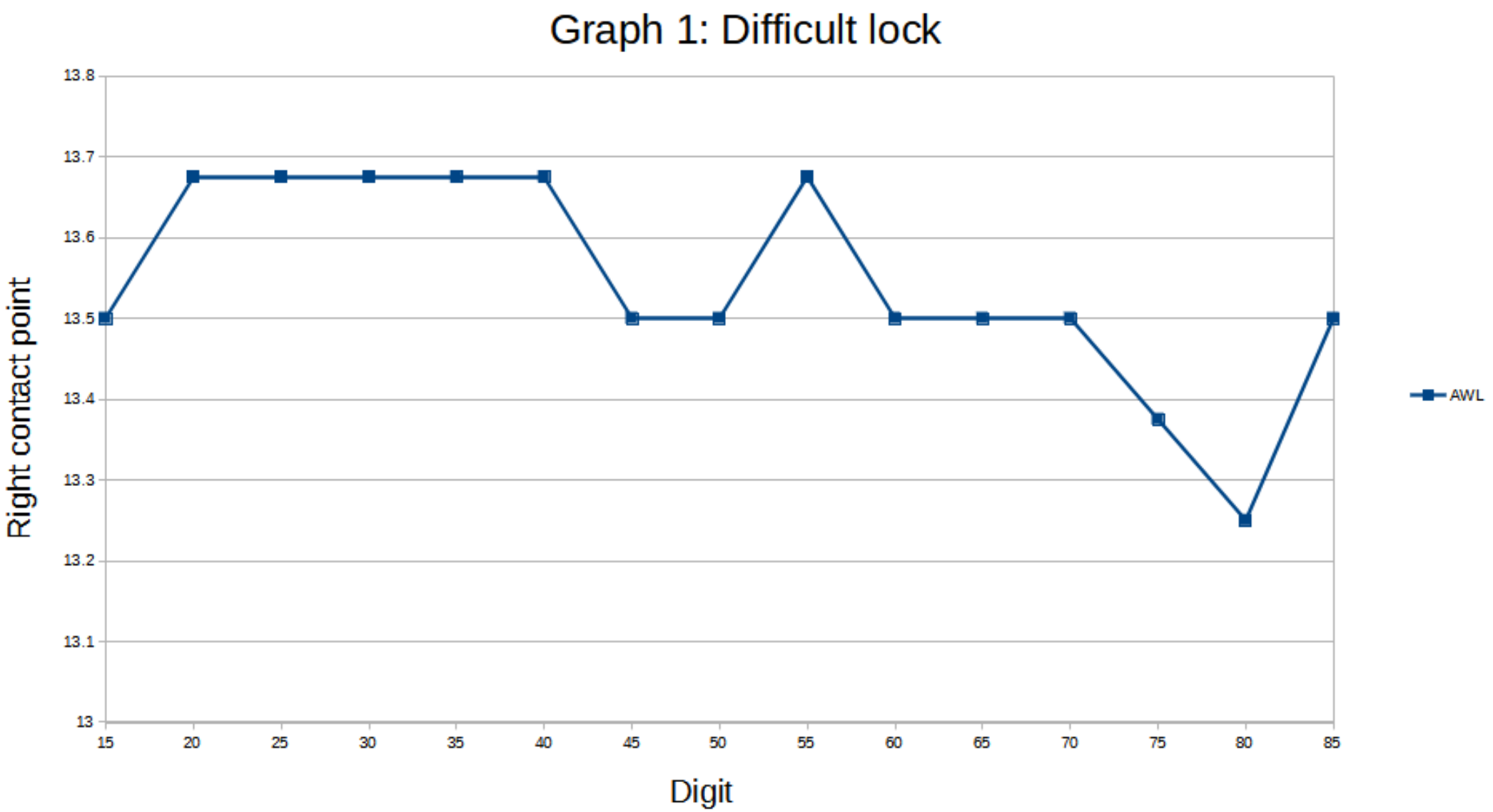
- Brute force the last number or make another graph.
- Brute forcing **L 50R 80L** the lock opened at **20**, giving us the solution **20L 50R 80L**.

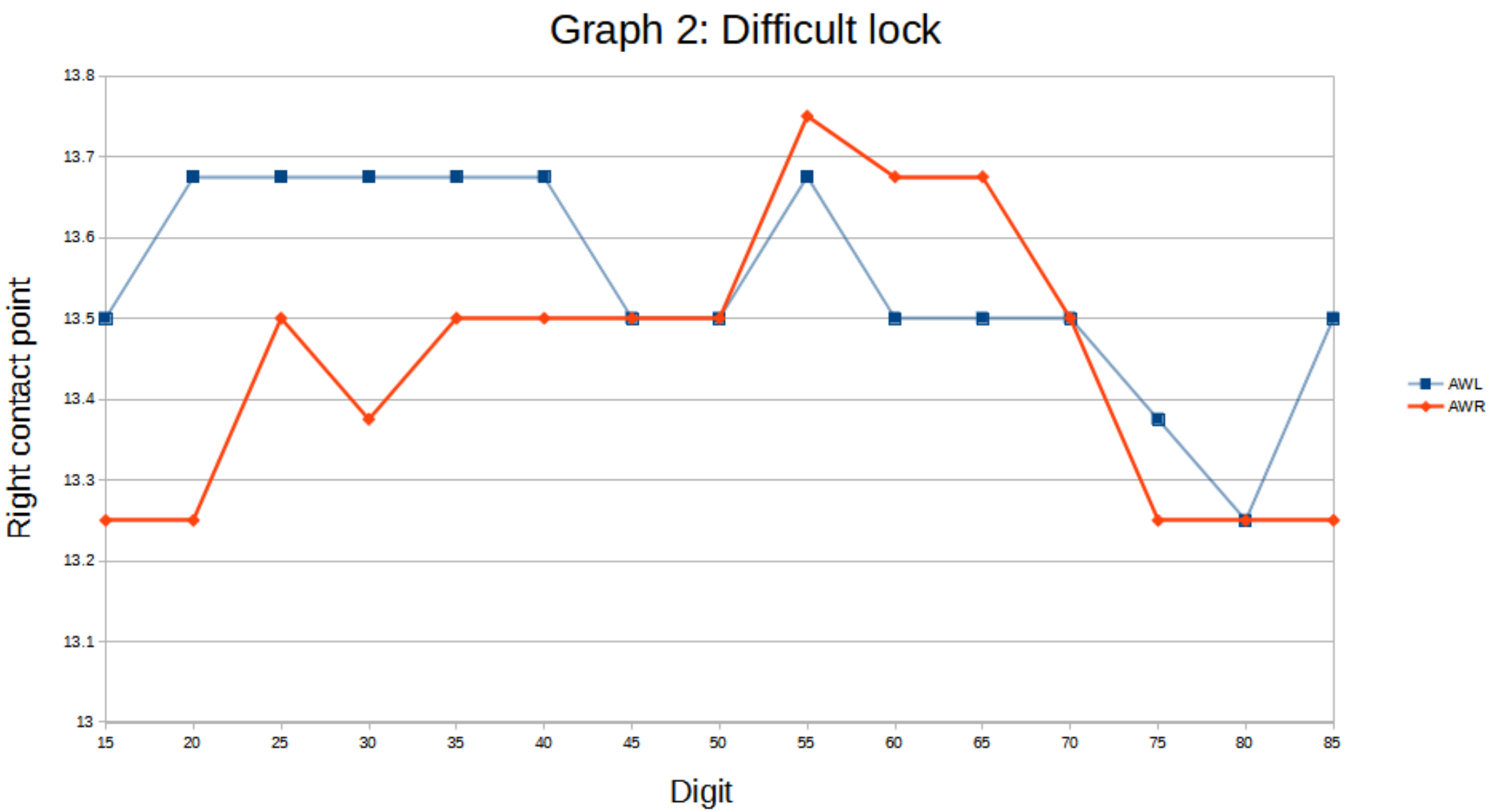
Manipulation process

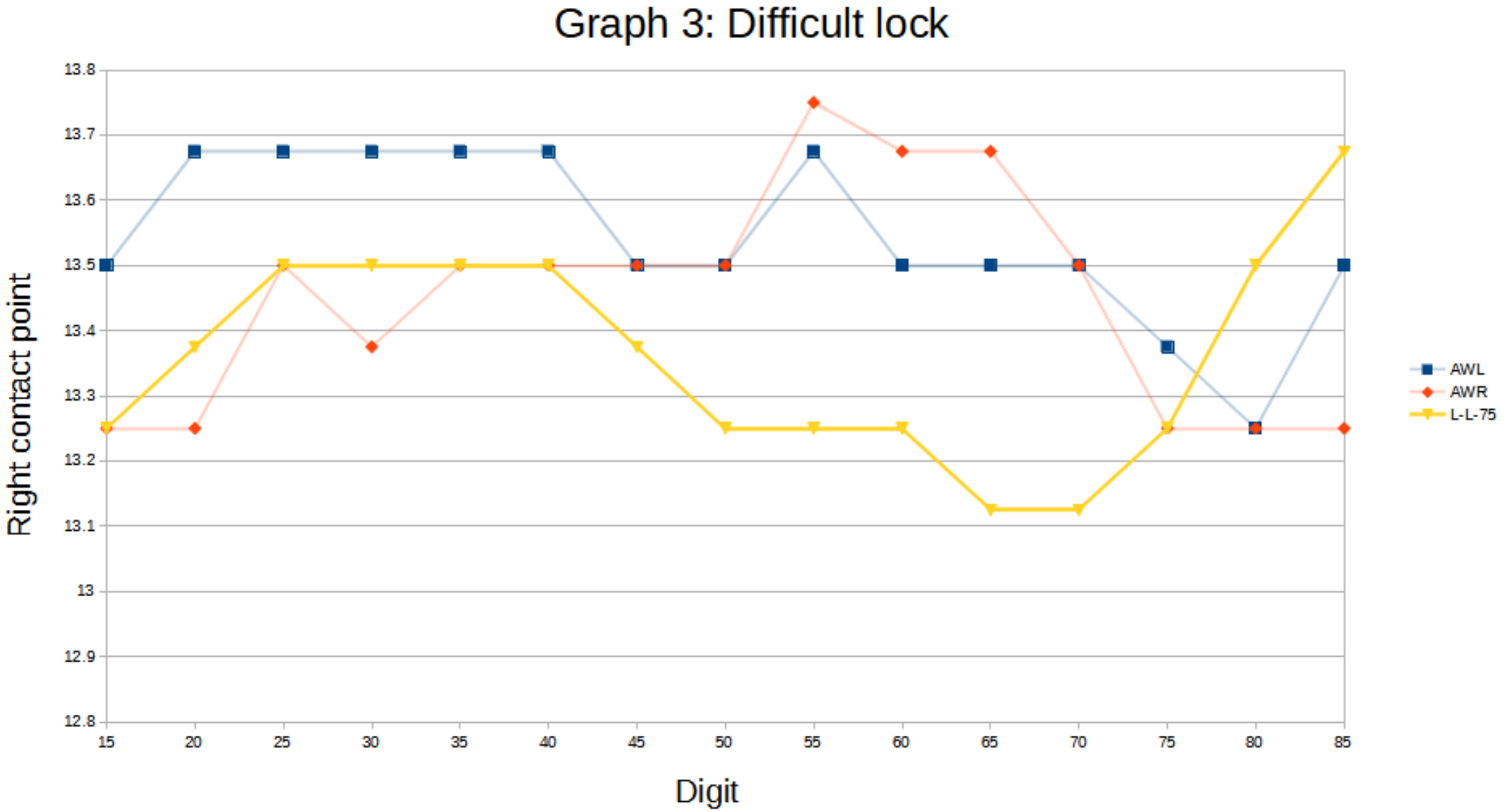
- Note the dialing direction
- Check every **n** numbers
- Be consistent in dialing/graphing
- Progress:
  - new low reading, this does not have to be a gate.

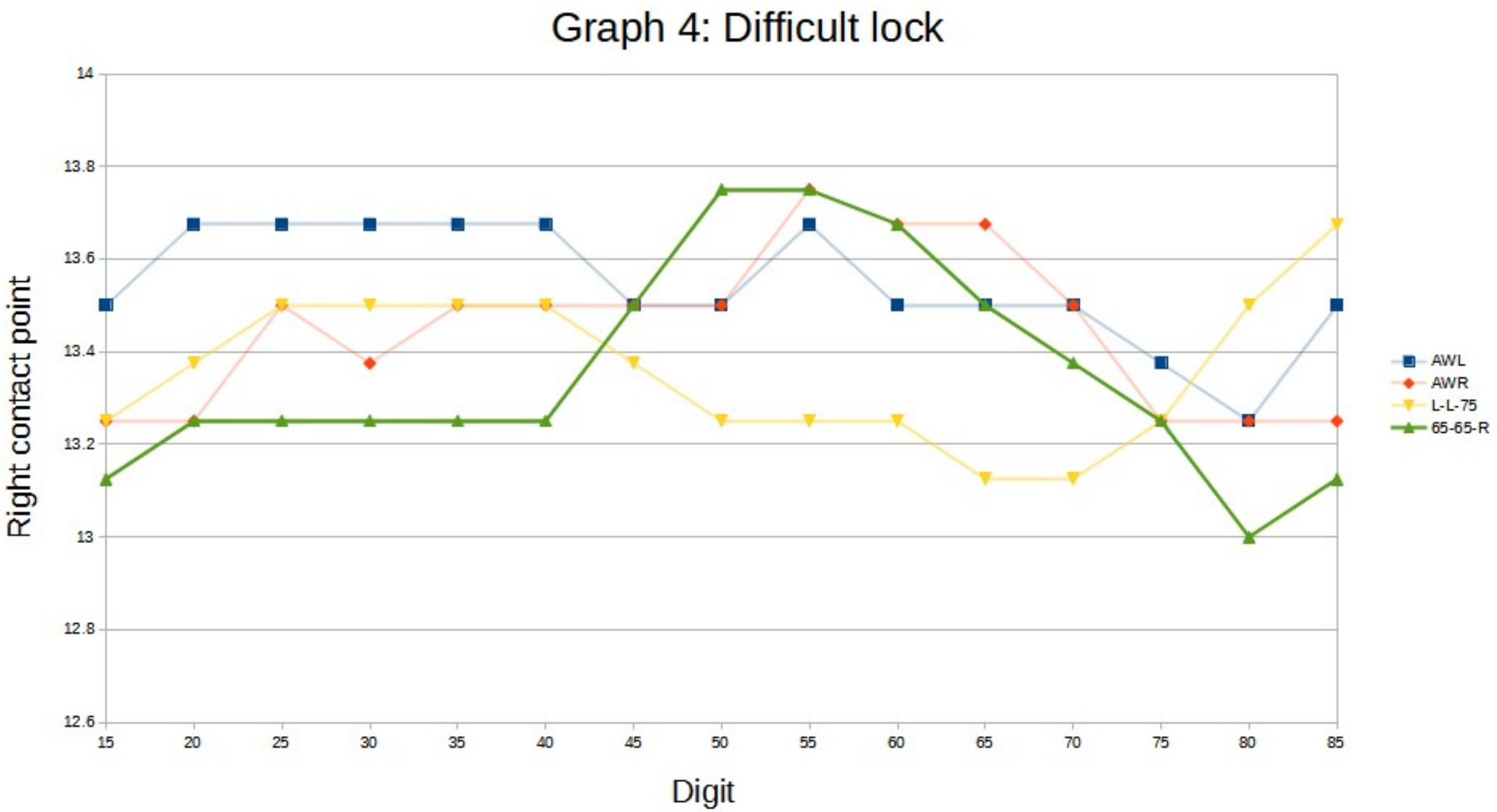
Manipulation process

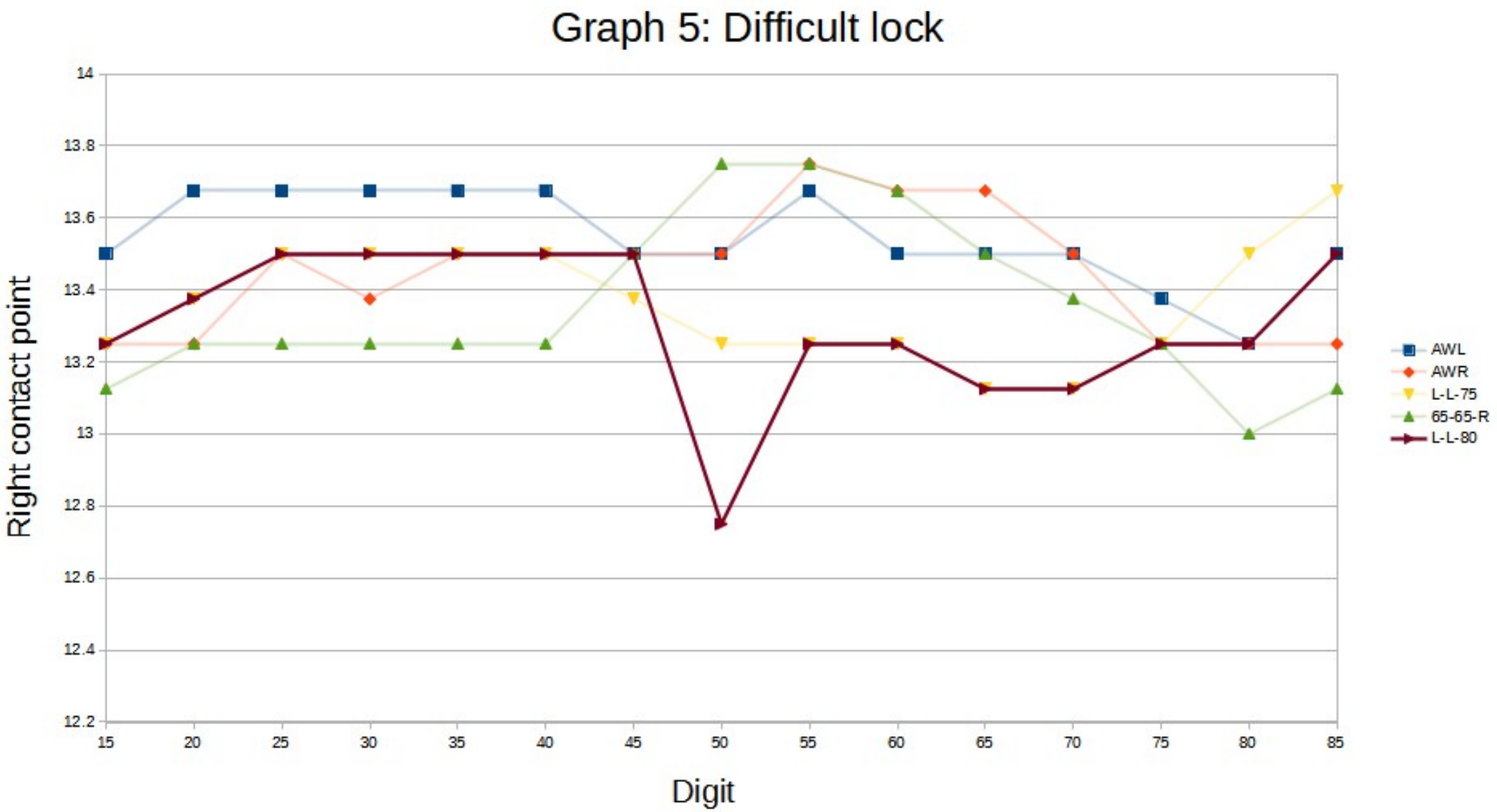
- Example graph of a harder lock.


Graph 1: Difficult lock
Right contact point
13.8
13.7
13.6
13.5
13.4
13.3
13.2
13.1
13
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Digit
AWL

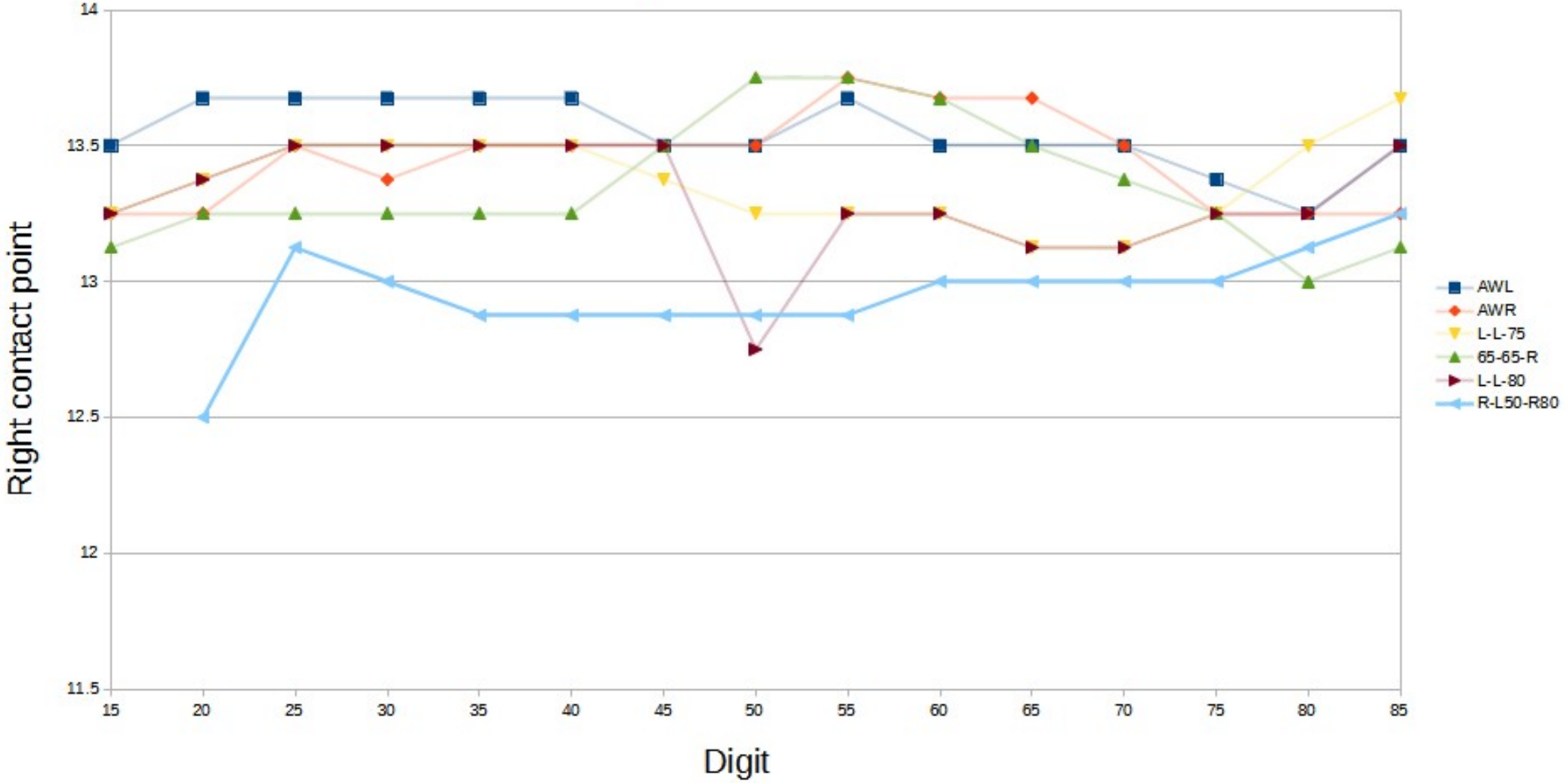

Graph 2: Difficult lock
Right contact point
13.8
13.7
13.6
13.5
13.4
13.3
13.2
13.1
13
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Digit
AWL
AWR


Graph 3: Difficult lock
Right contact point
13.8
13.7
13.6
13.5
13.4
13.3
13.2
13.1
13
12.9
12.8
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Digit
AWL
AWR
L-L-75


Graph 4: Difficult lock
Right contact point
14
13.8
13.6
13.4
13.2
13
12.8
12.6
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Digit
AWL
AWR
L-L-75
65-65-R


Graph 5: Difficult lock
Right contact point
14
13.8
13.6
13.4
13.2
13
12.8
12.6
12.4
12.2
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Digit
AWL
AWR
L-L-75
65-65-R
L-L-80

Graph 6: Difficult lock

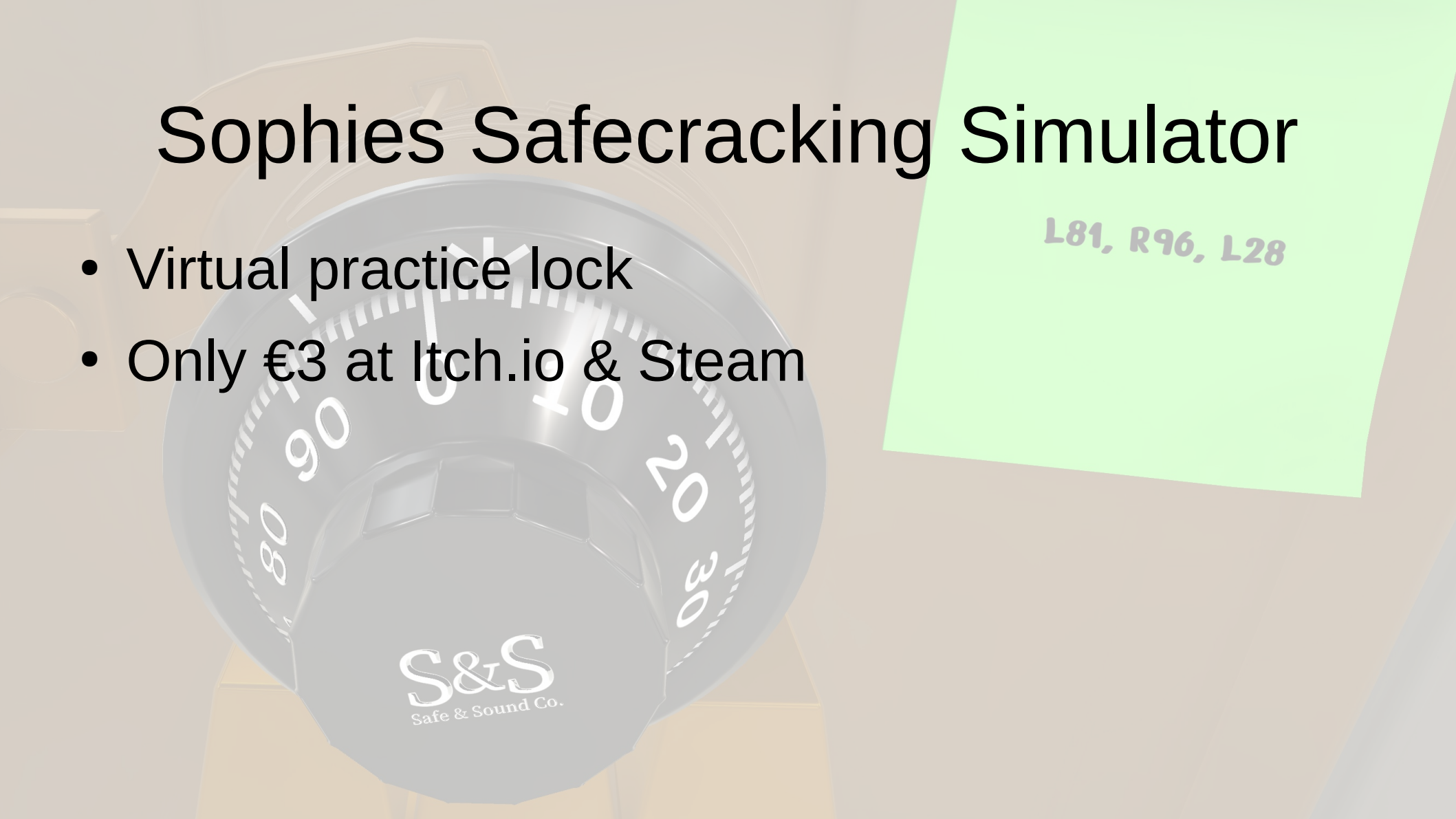


Manipulation process

- Don’t give up: Each graph got us closer to open

Sophies Safecracking Simulator

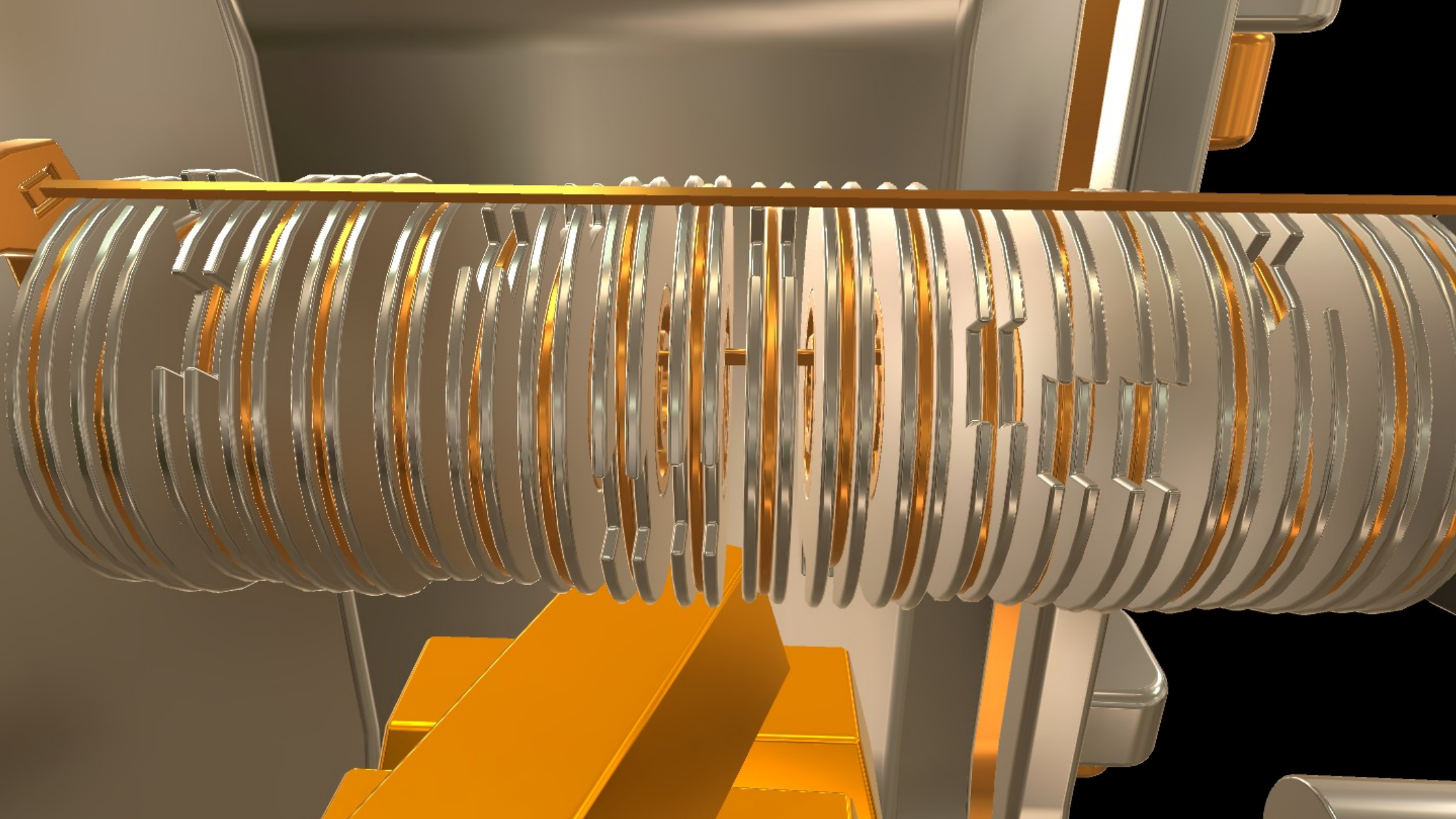
- Virtual practice lock
- Only €3 at Itch.io & Steam

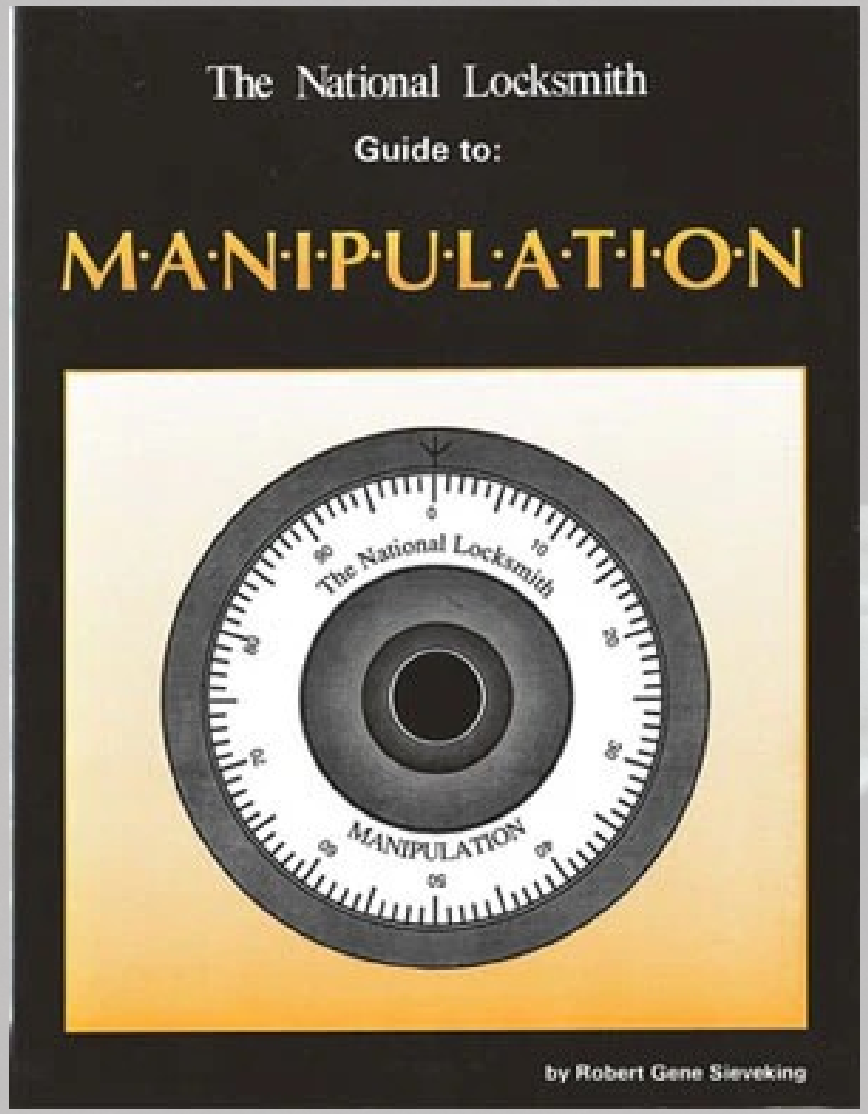


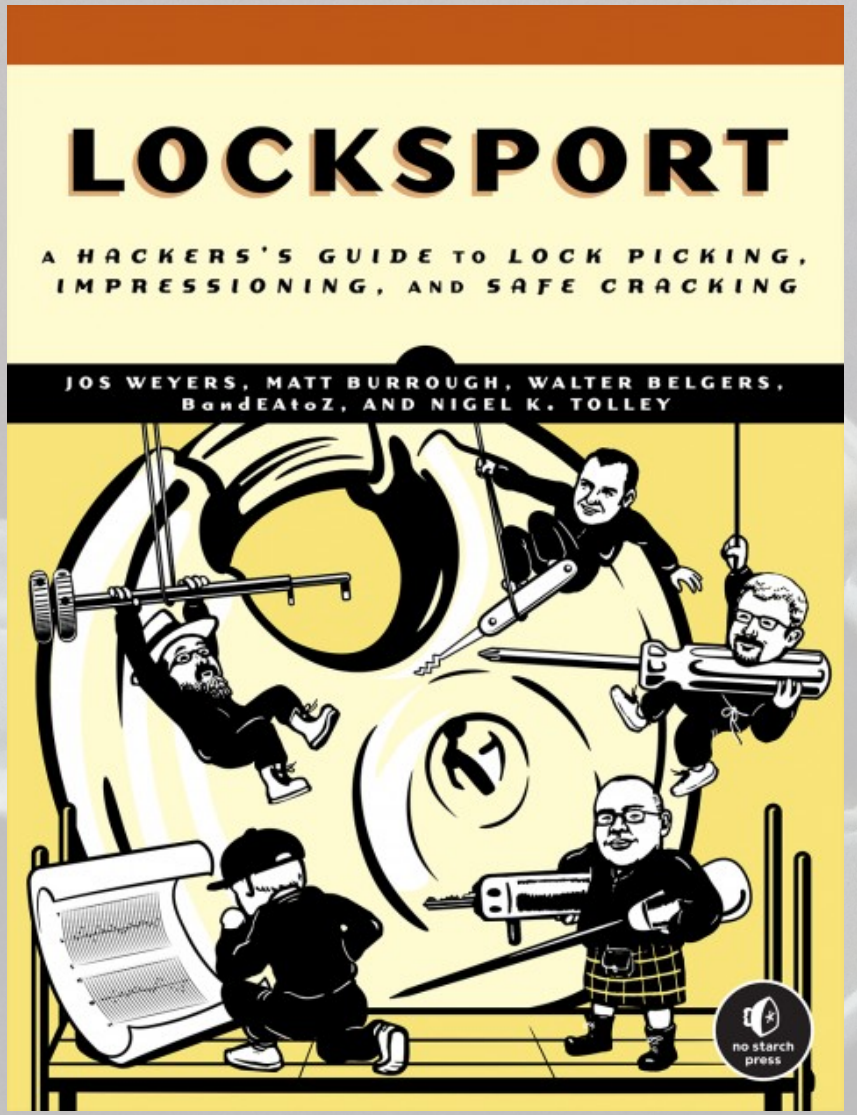
Virtual lock to practice

- Play
- Change Lock
- Tutorial
- Settings
- Credits
- Quit Game


36,400
0
10
20
30
40
06
Wi-Fi GyBro




The National Locksmith
Guide to:
M·A·N·I·P·U·L·A·T·I·O·N
The National Locksmith
MANIPULATION
by Robert Gene Sieveking


LOCKSPORT
A HACKER'S GUIDE TO LOCK PICKING, IMPRESSIONING, AND SAFE CRACKING
JOS WEYERS, MATT BURROUGH, WALTER BELGERS, BandEAtoZ, AND NIGEL K. TOLLEY
no starch press

The end

- Question →
  - Lockpicking village next to Clairvoyance
- Contact:

Jan-willem@Toool.nl

@jwrm22