

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

Jan-Willem
May Contain Hackers 2022

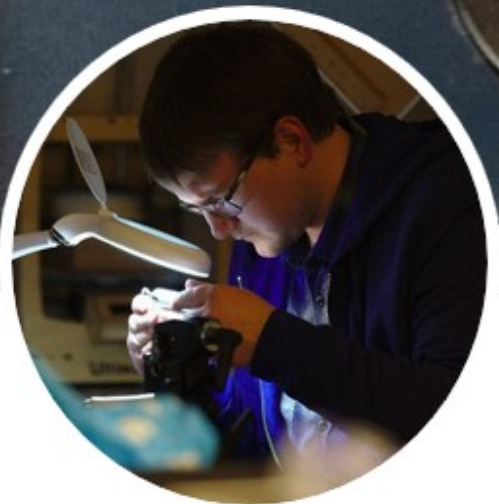
What if locks could talk; what stories would they tell?

- Talking with locks?
- History
- Side channels

Binel

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.

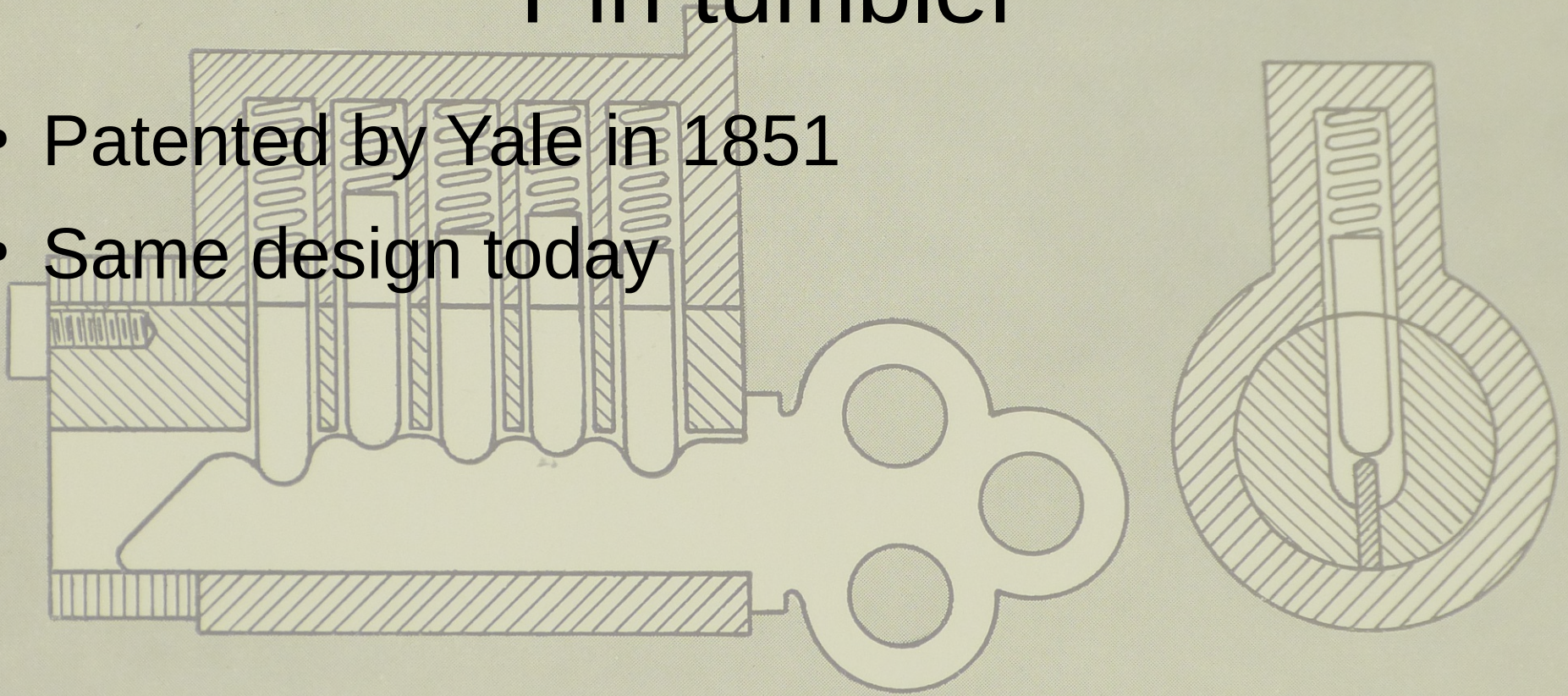
Rules of Lockpicking

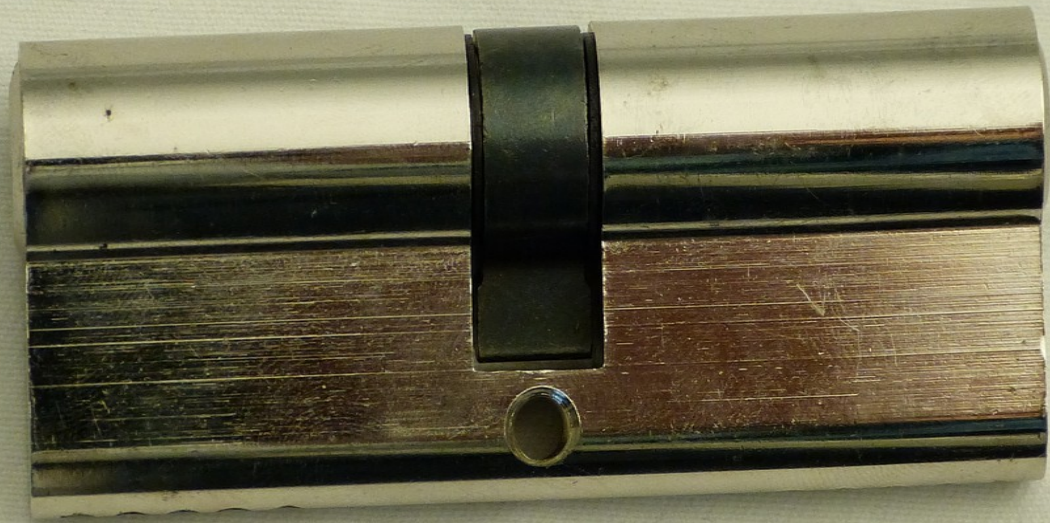
A background image showing various lockpicking tools, including tension wrenches and picks, arranged on a light-colored surface. The tools are slightly out of focus, creating a soft, artistic effect.

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

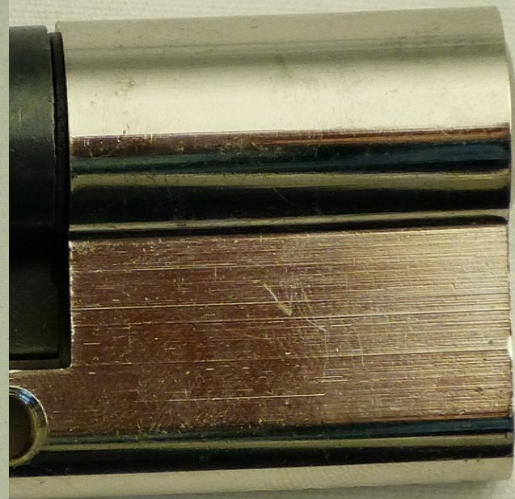
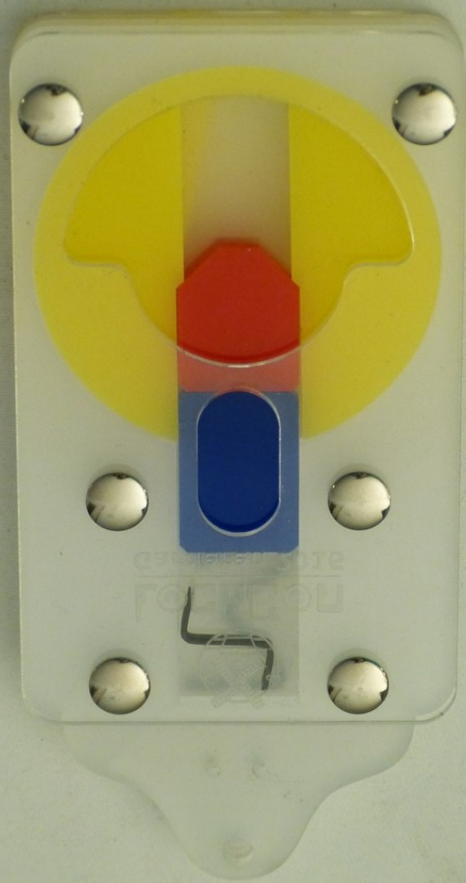
Pin tumbler

- Patented by Yale in 1851
- Same design today

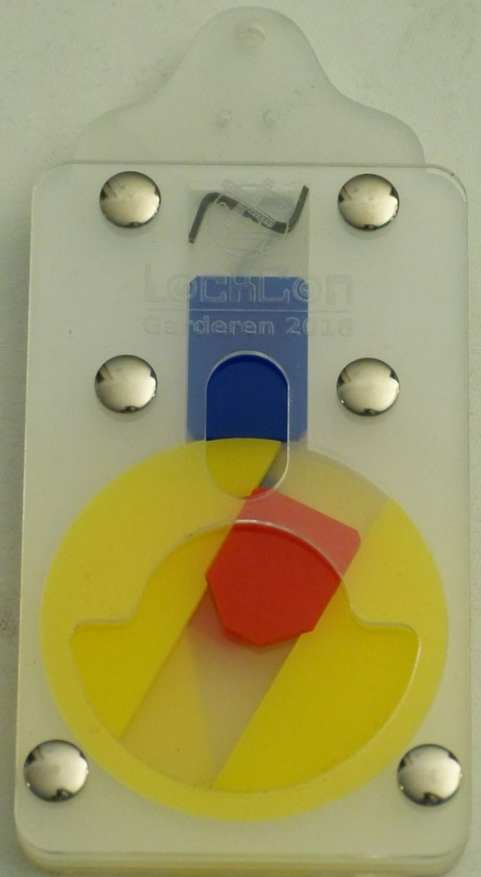
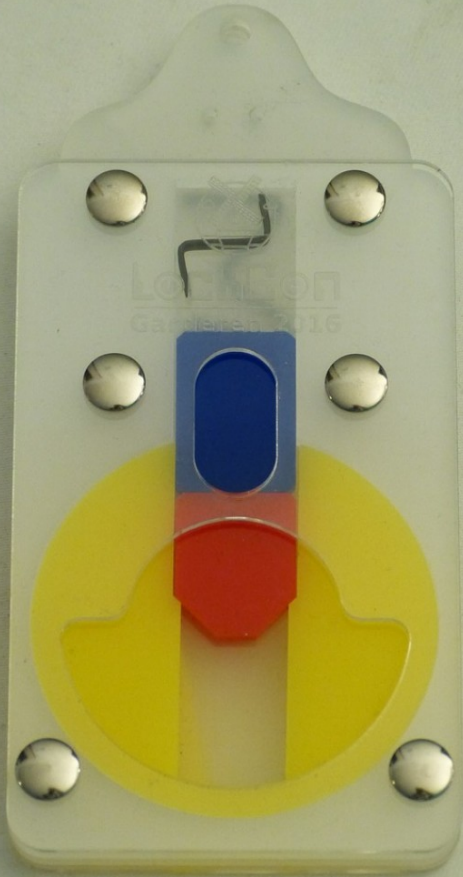




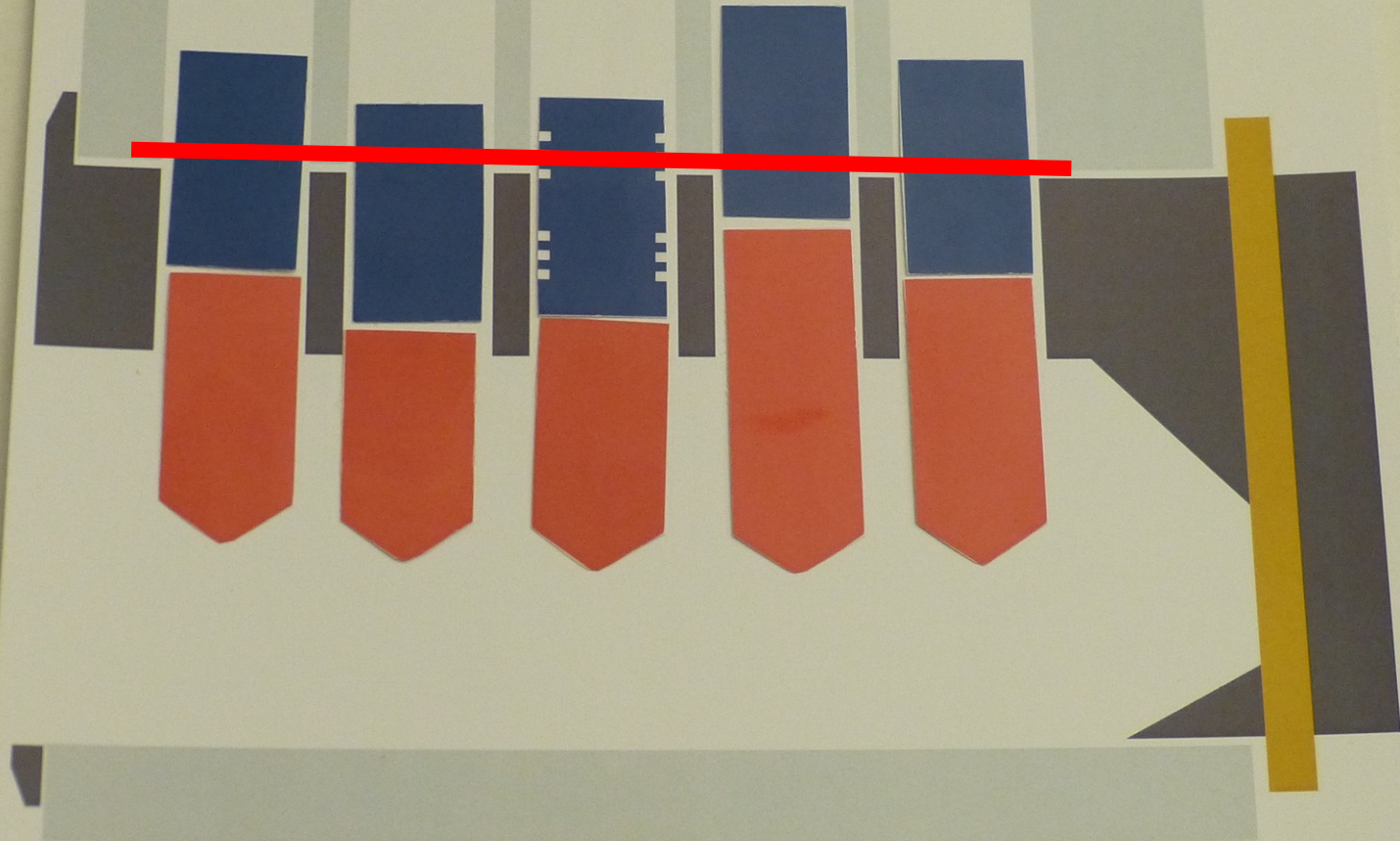
Orientation



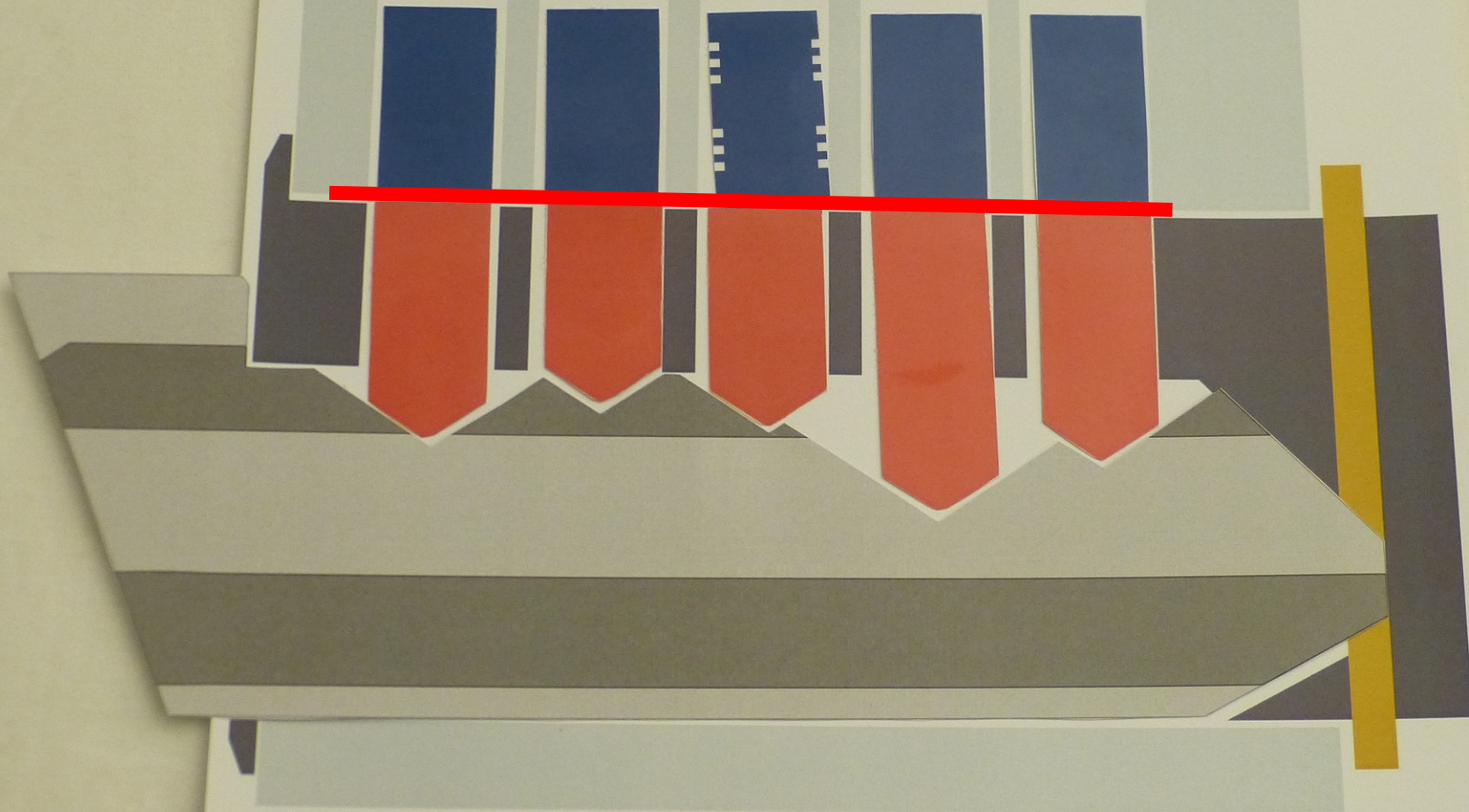
Locks



Without key



Correct key

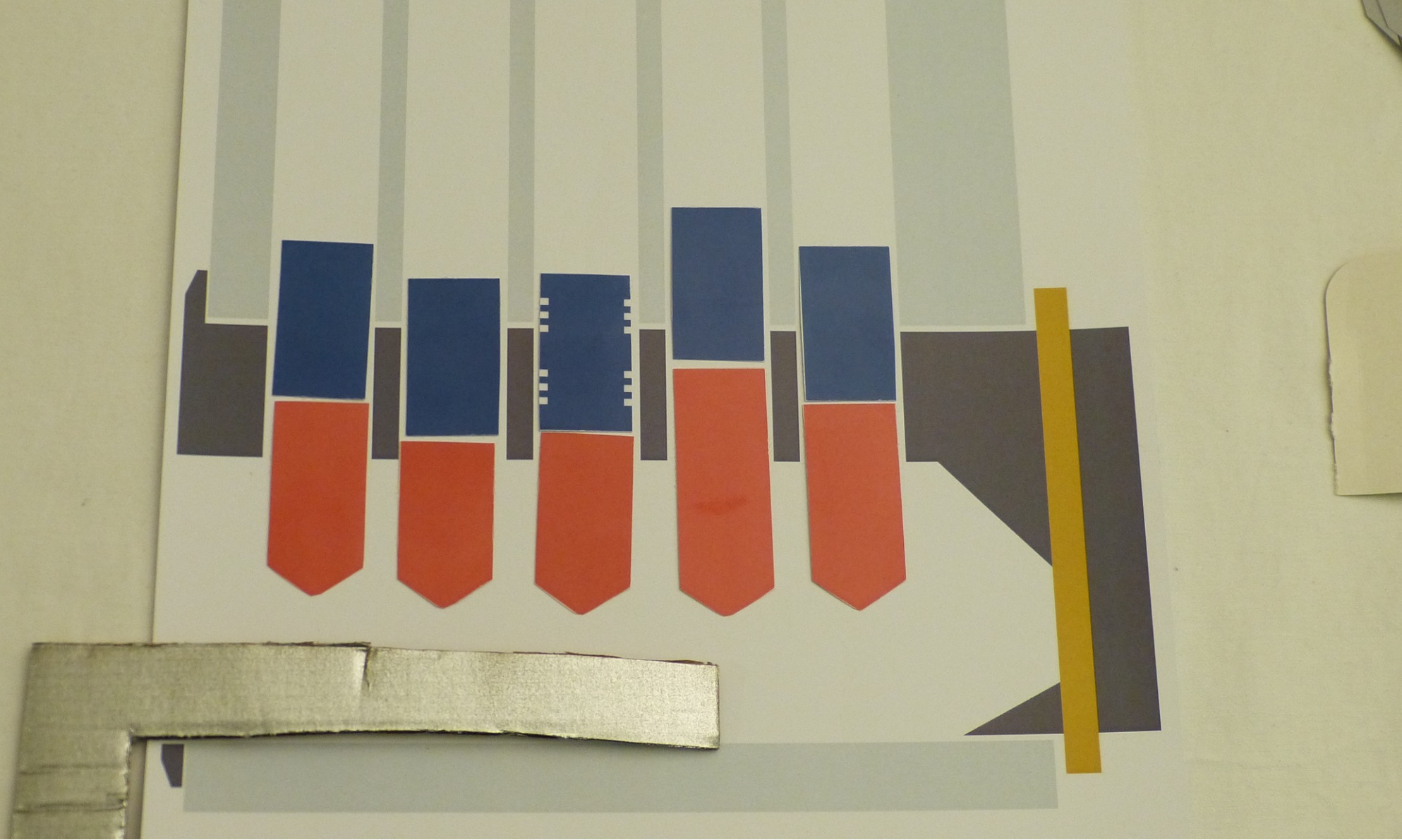


Wrong key



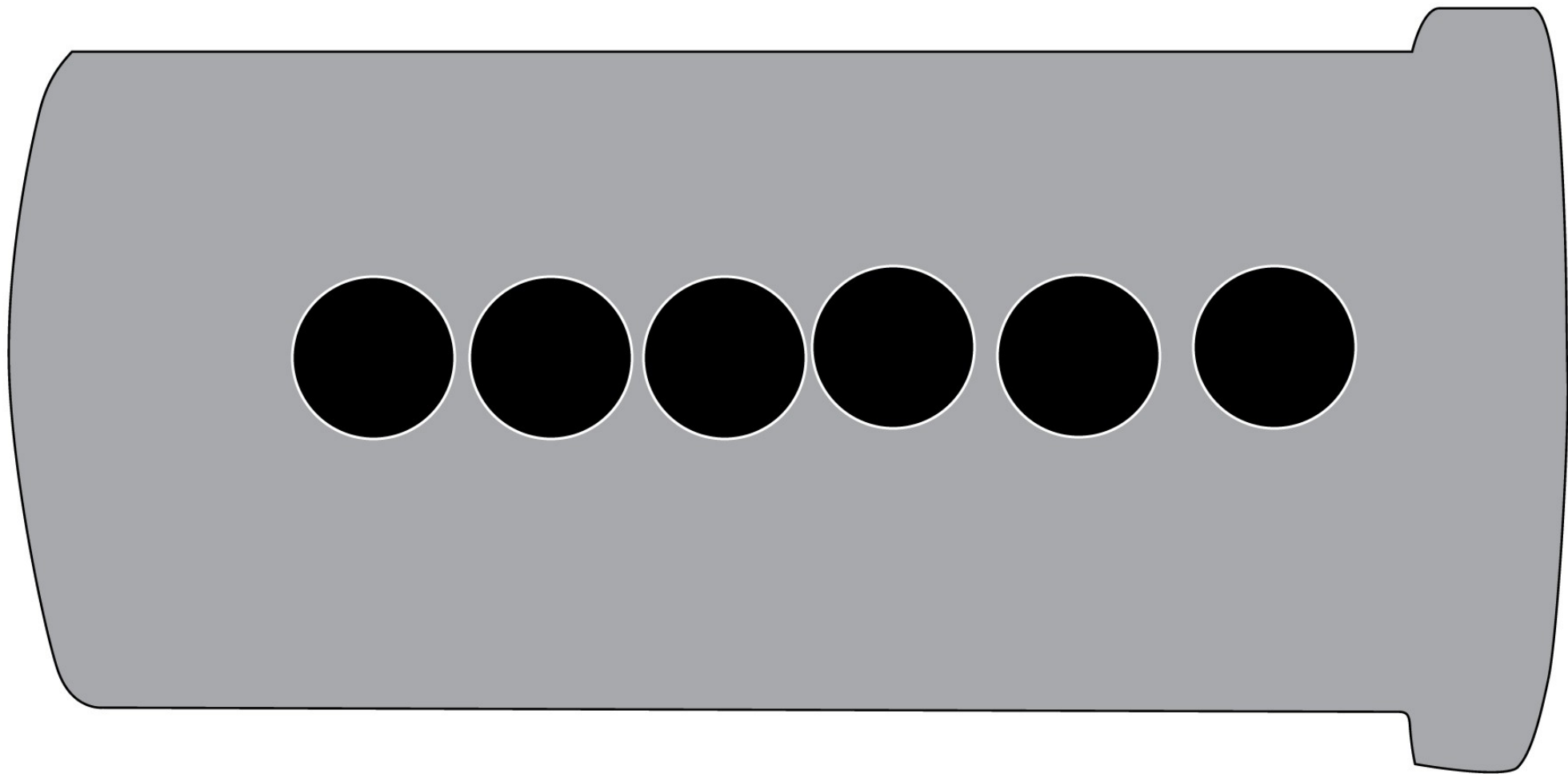
What are the side channels?

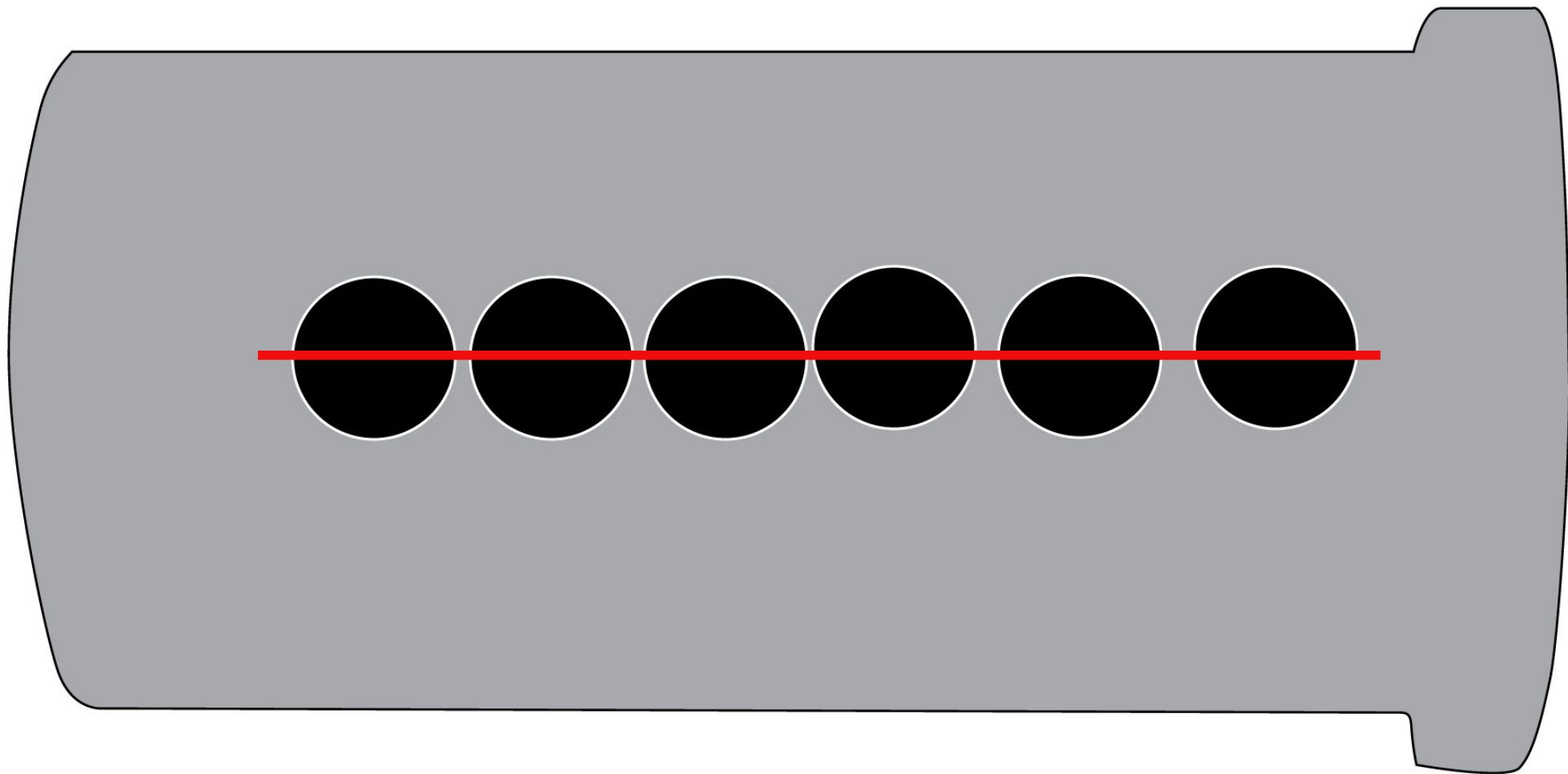
- Binding of the pins
- Rotation of the core
- ???



Binel

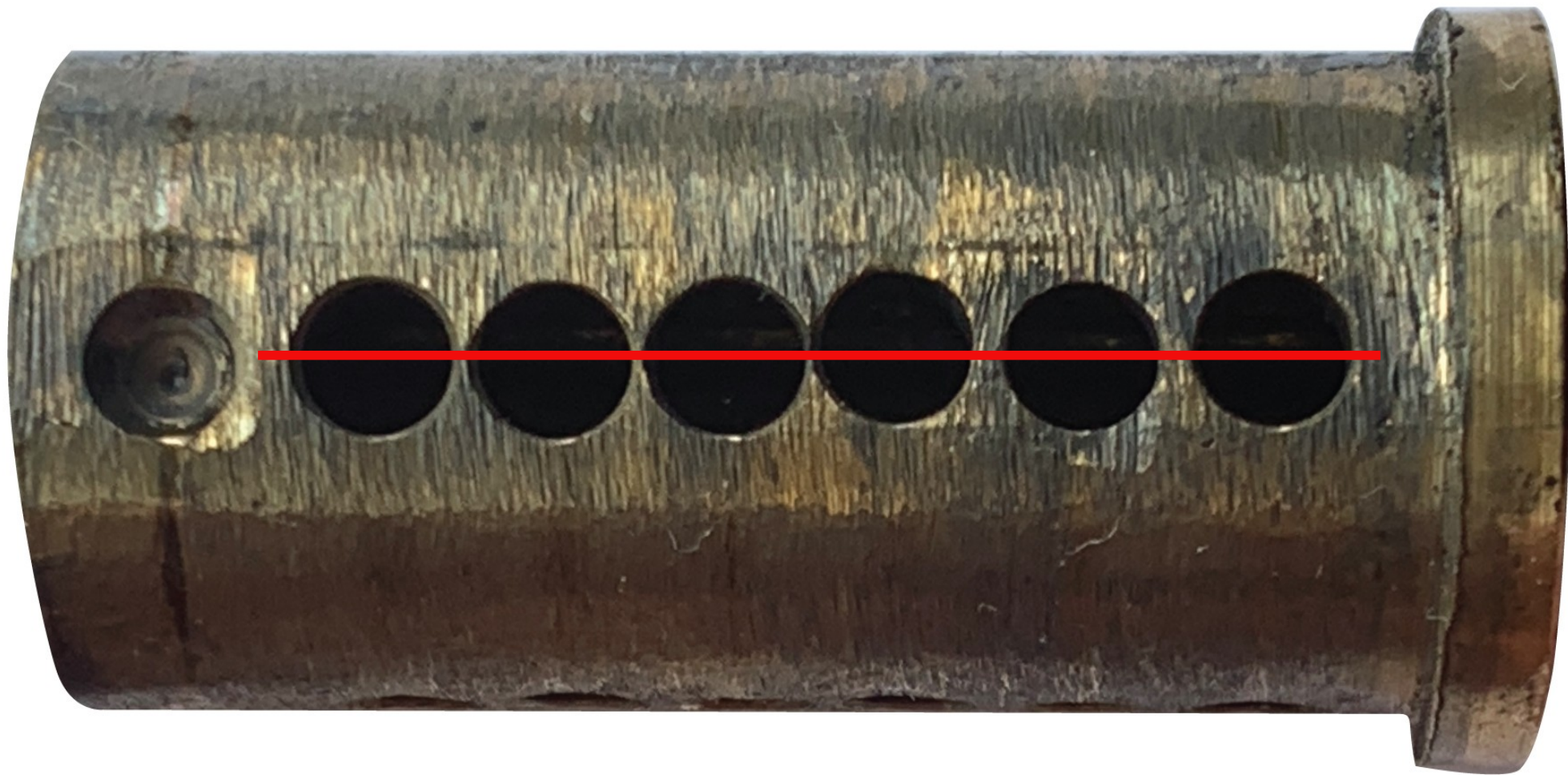






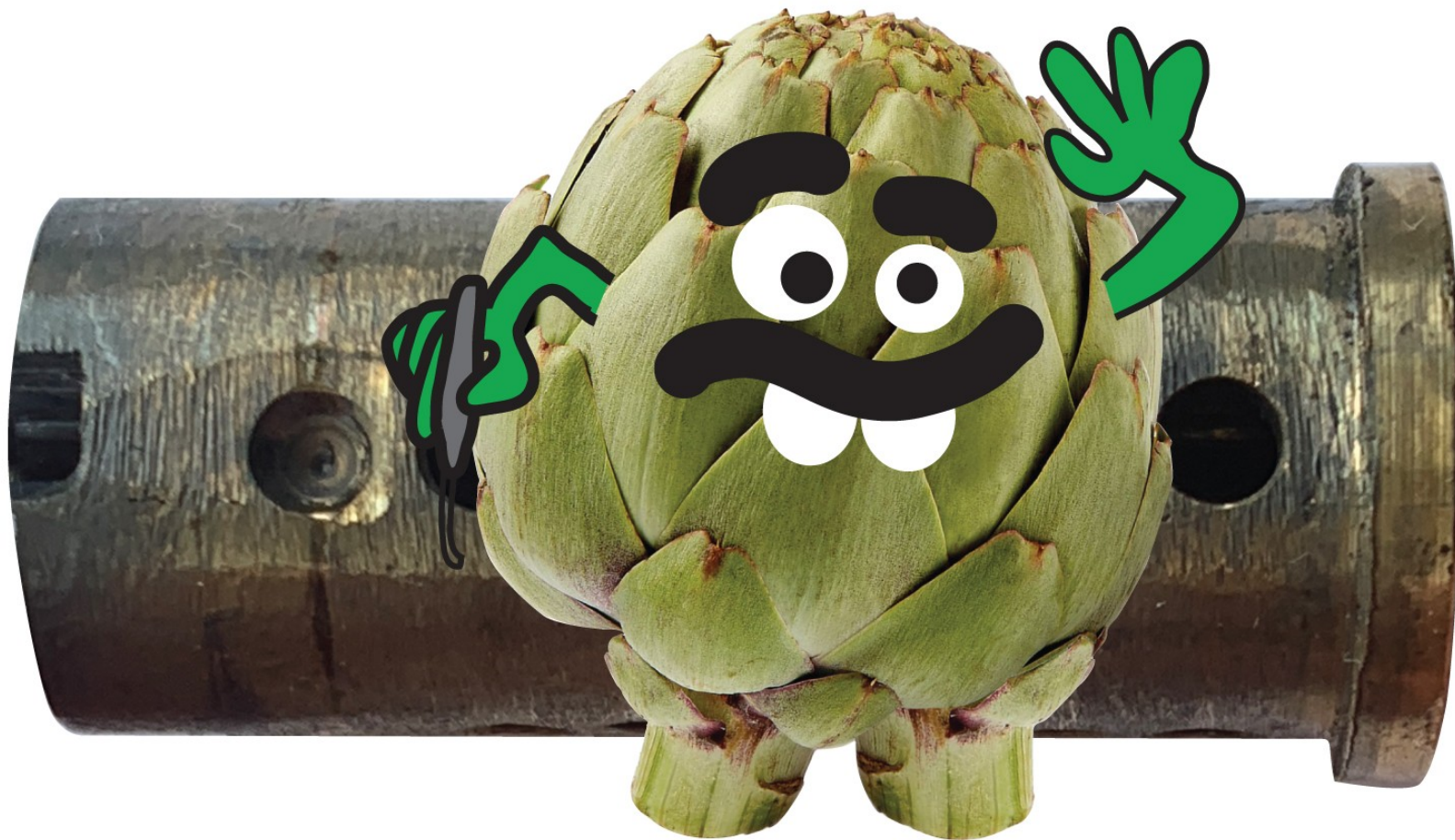
COURTESY ARTICHOKE2000





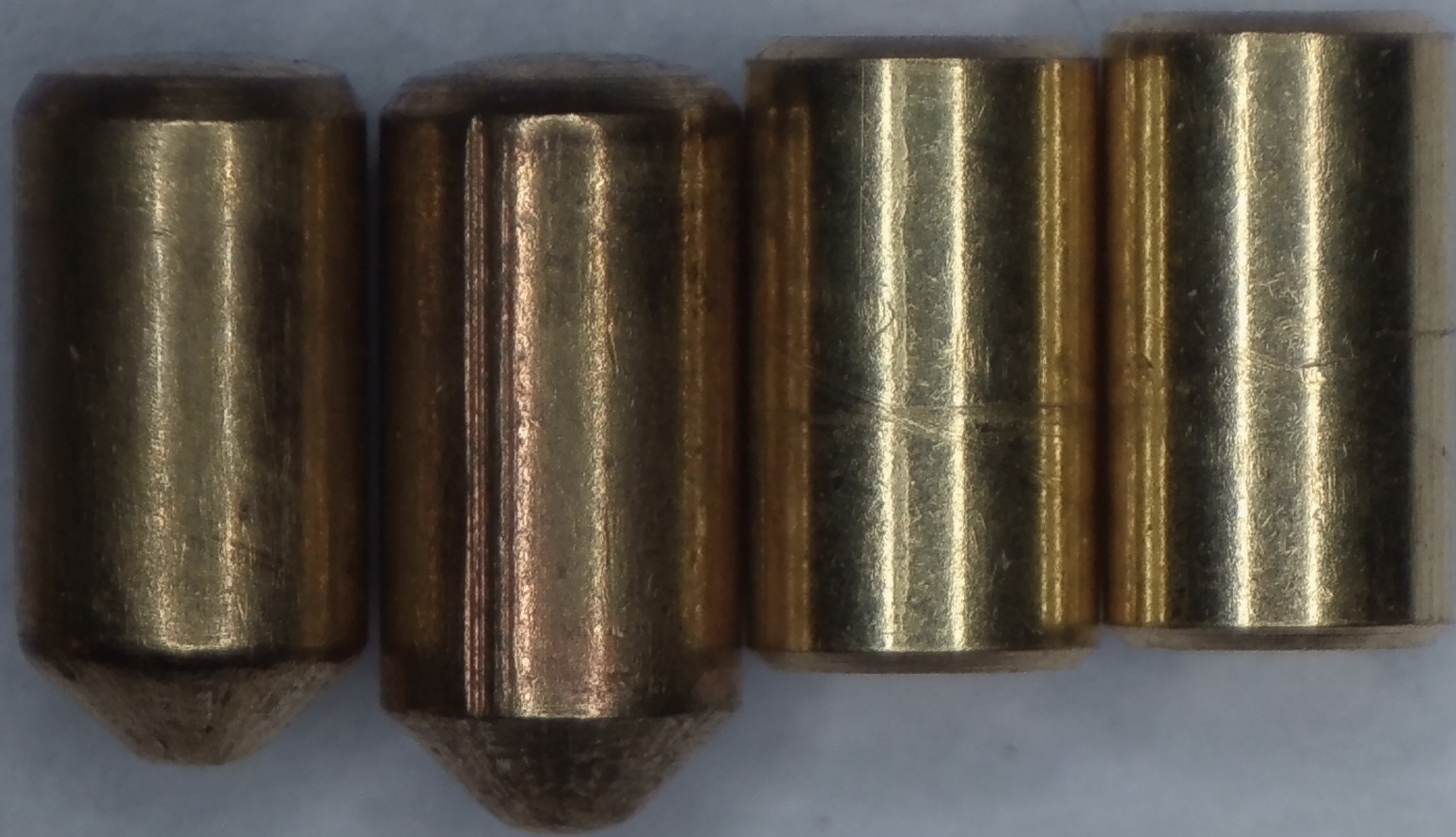
COURTESY ARTICHOKE2000

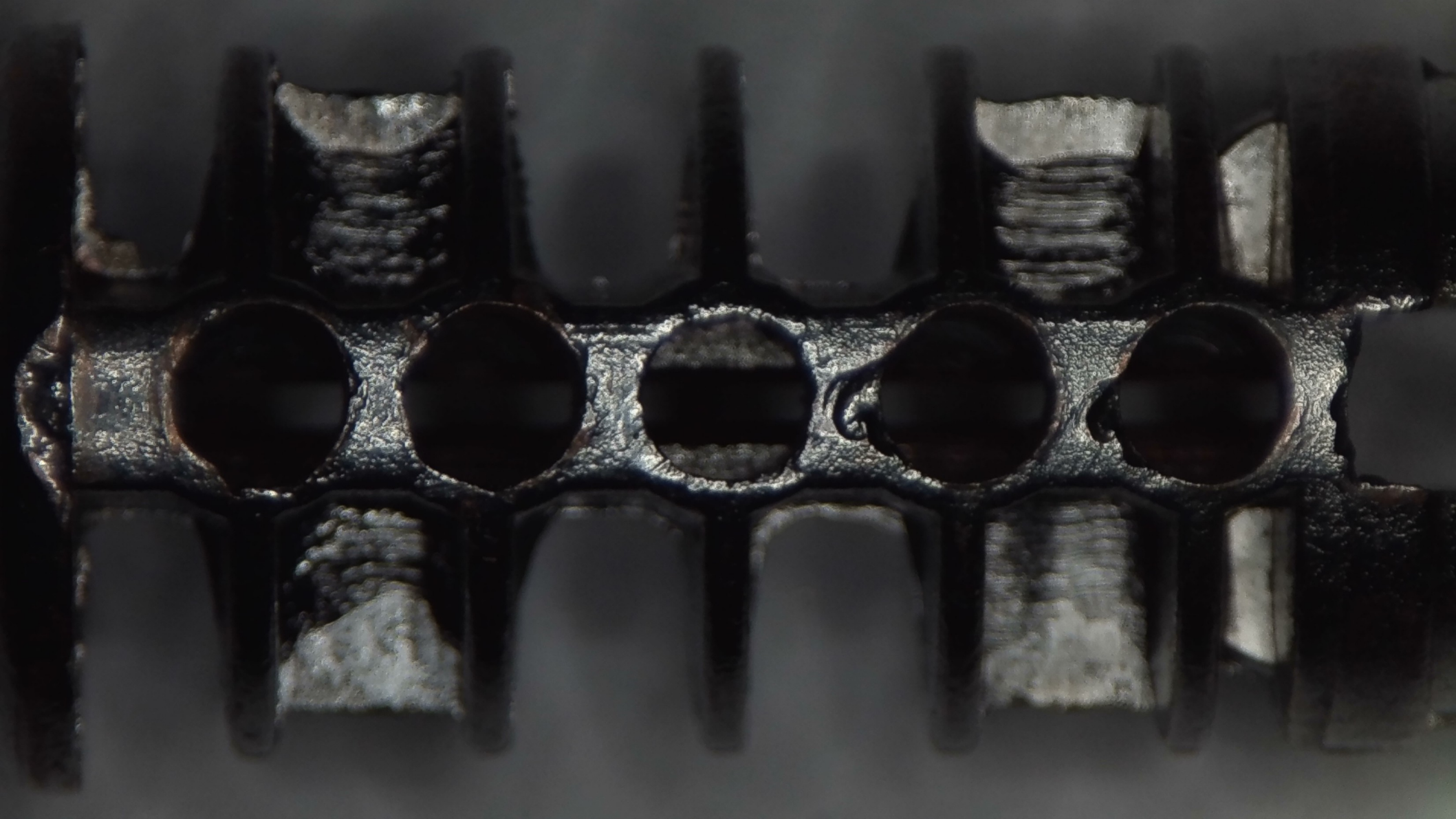




COURTESY ARTICHOKE2000









Lockpicking



Binel



Binel

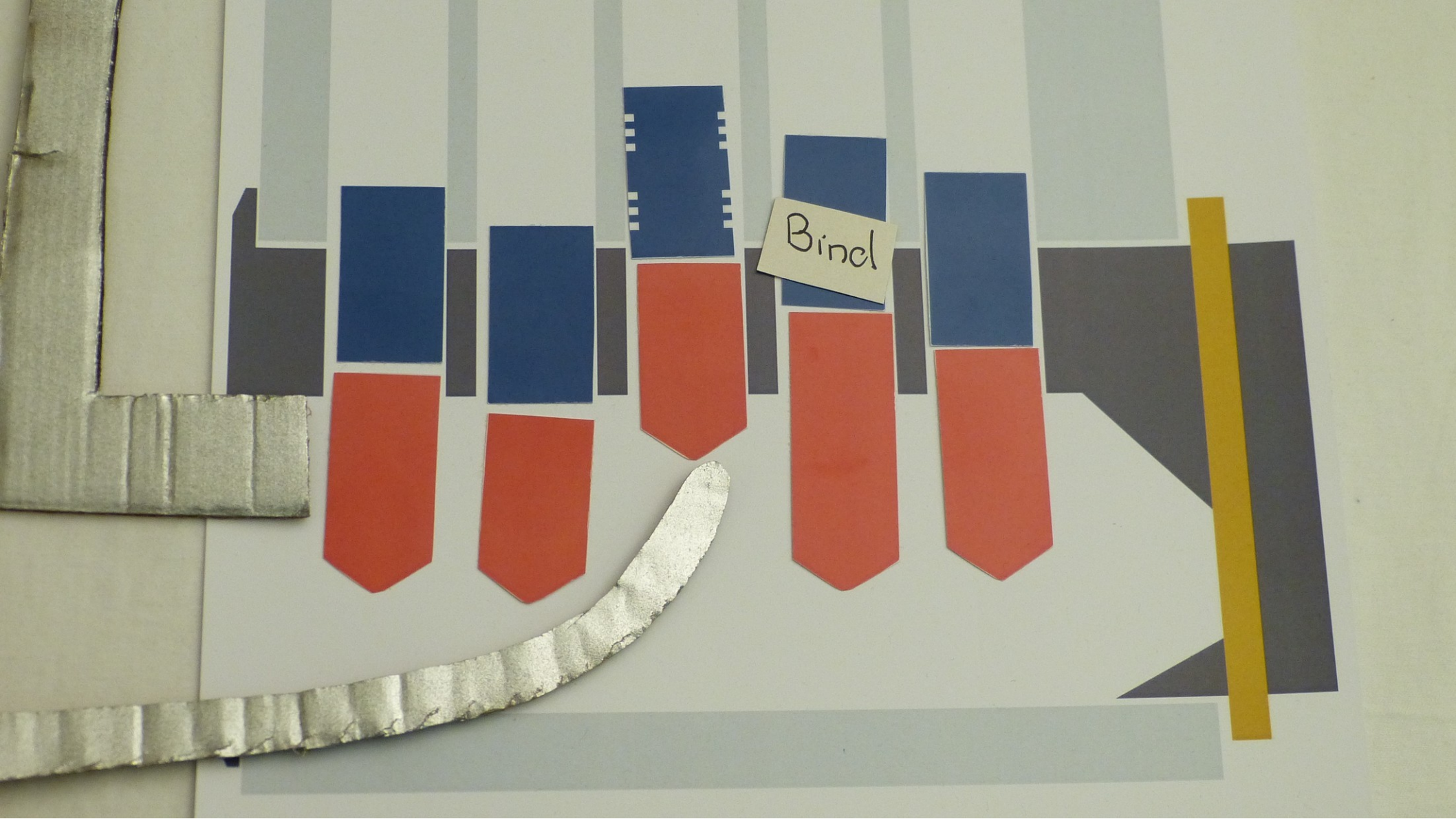


Binel



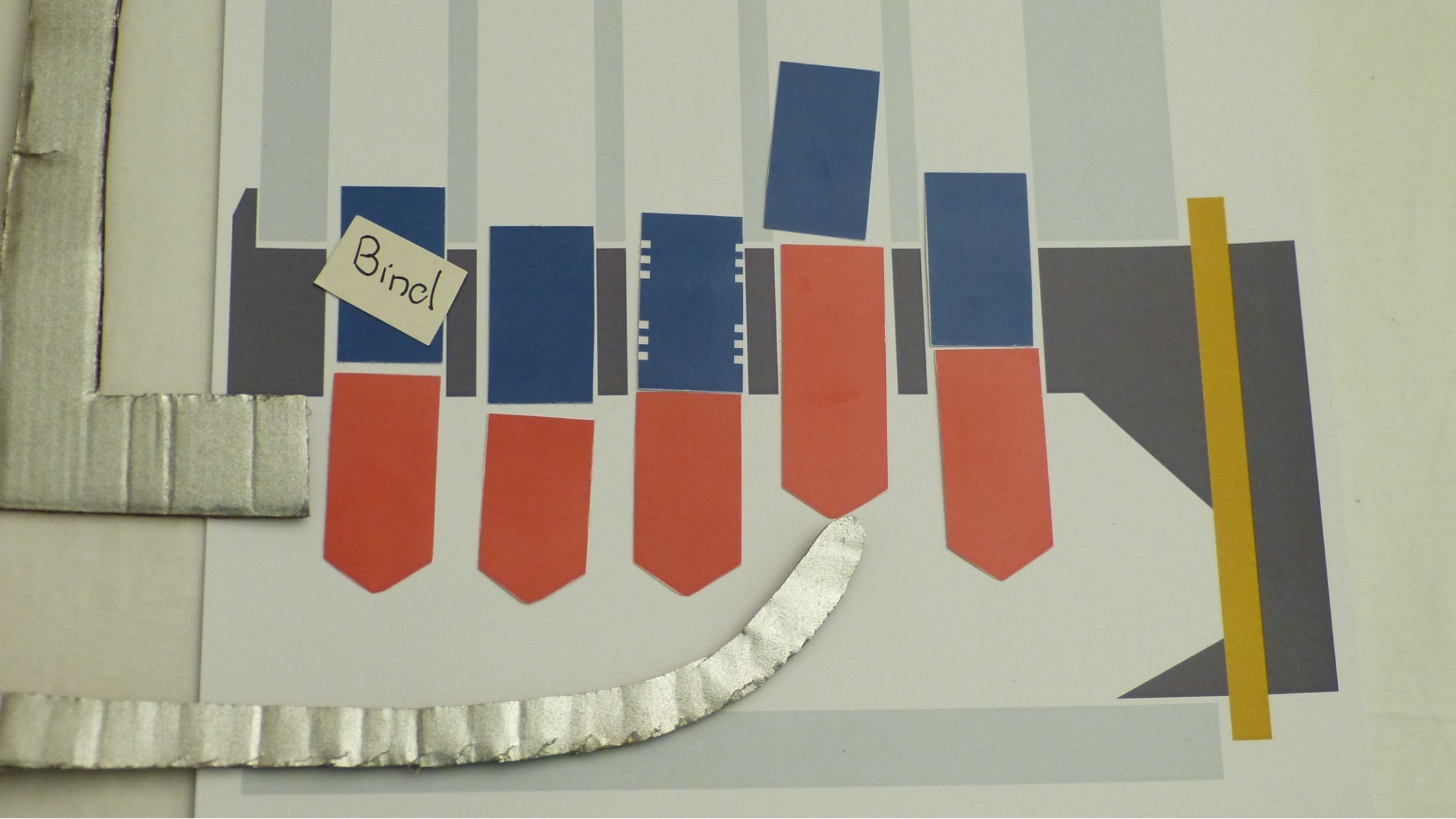


Binel



Binel

Binel



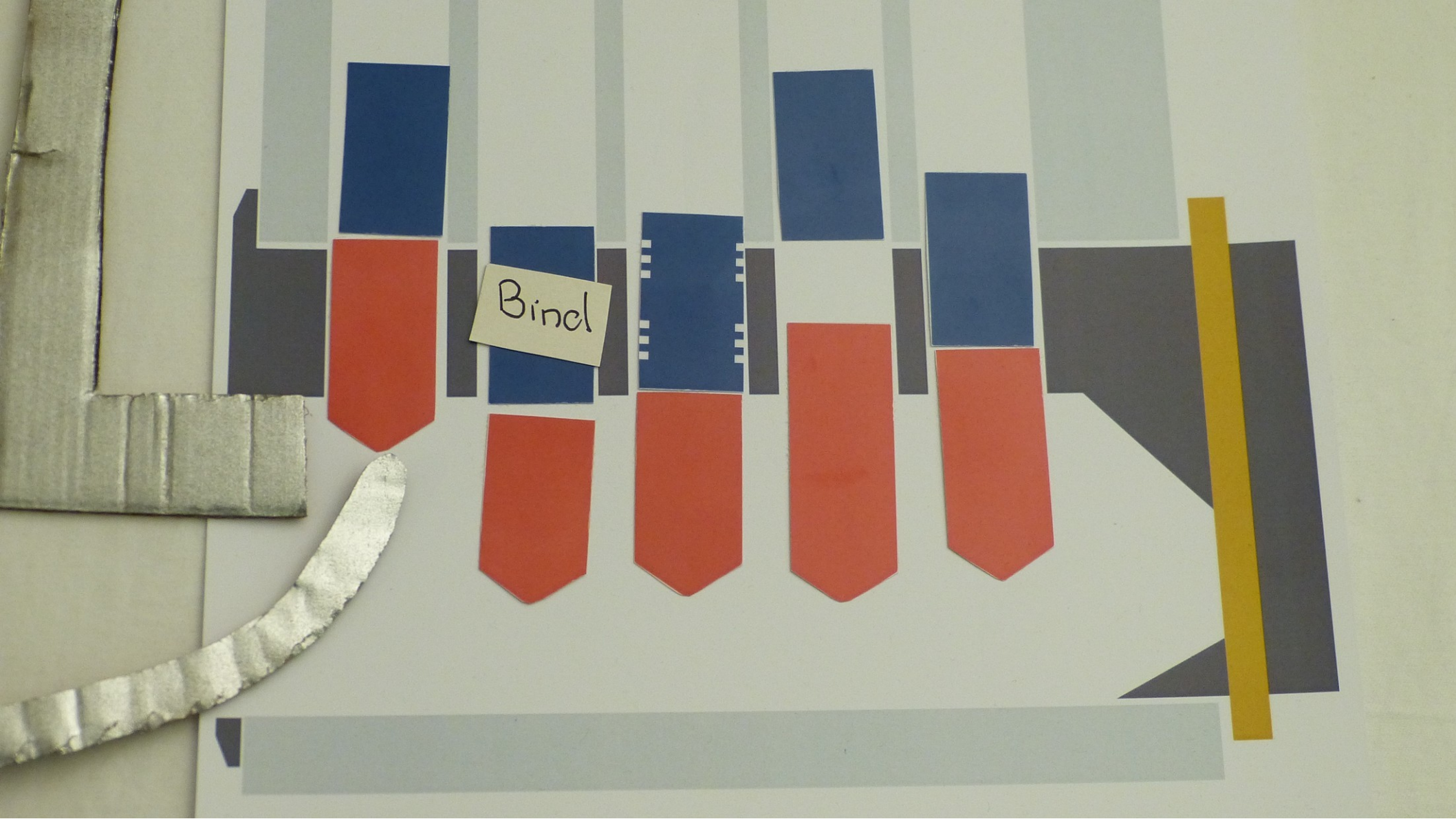
Binel

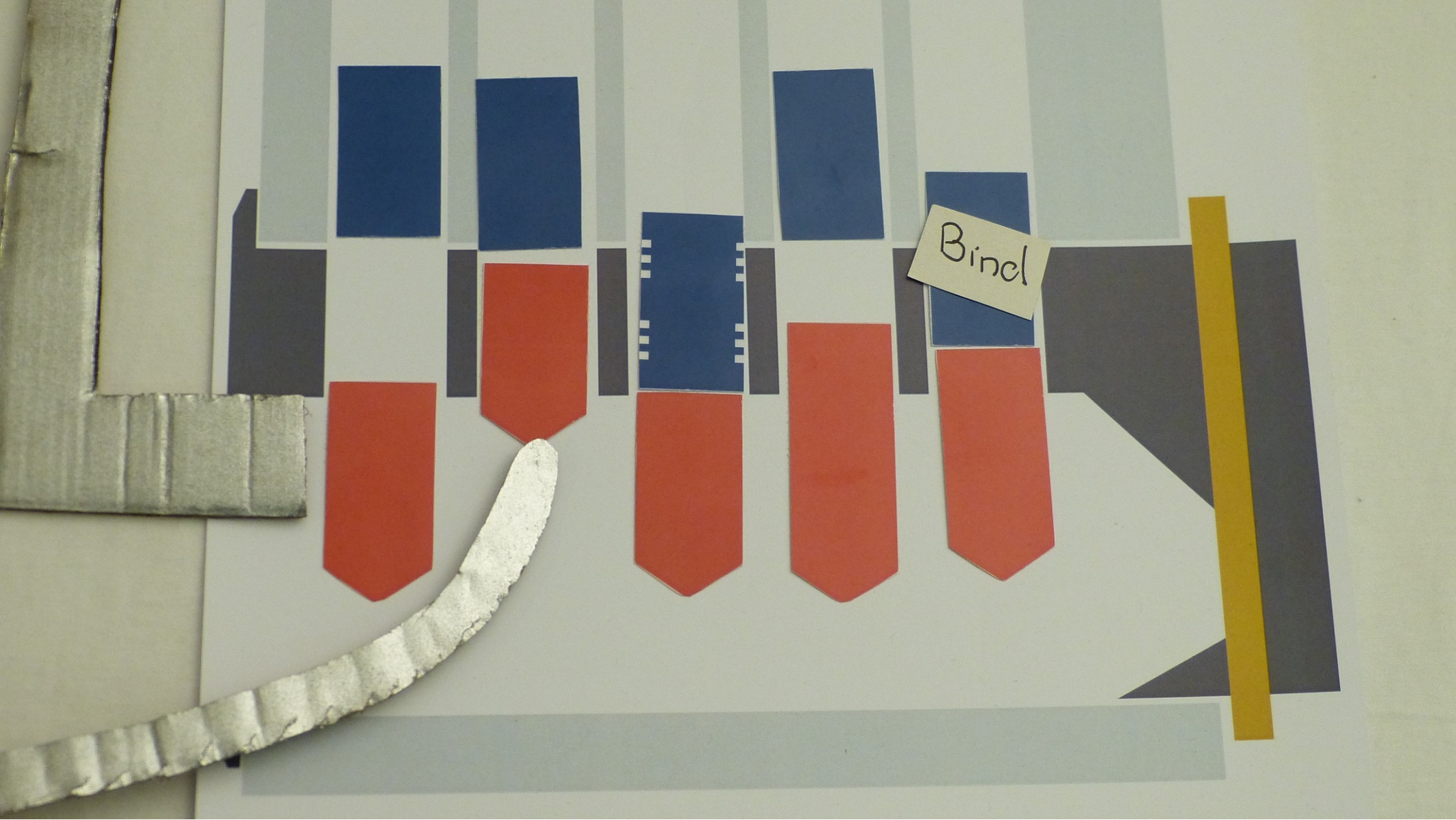


Binel



Binel



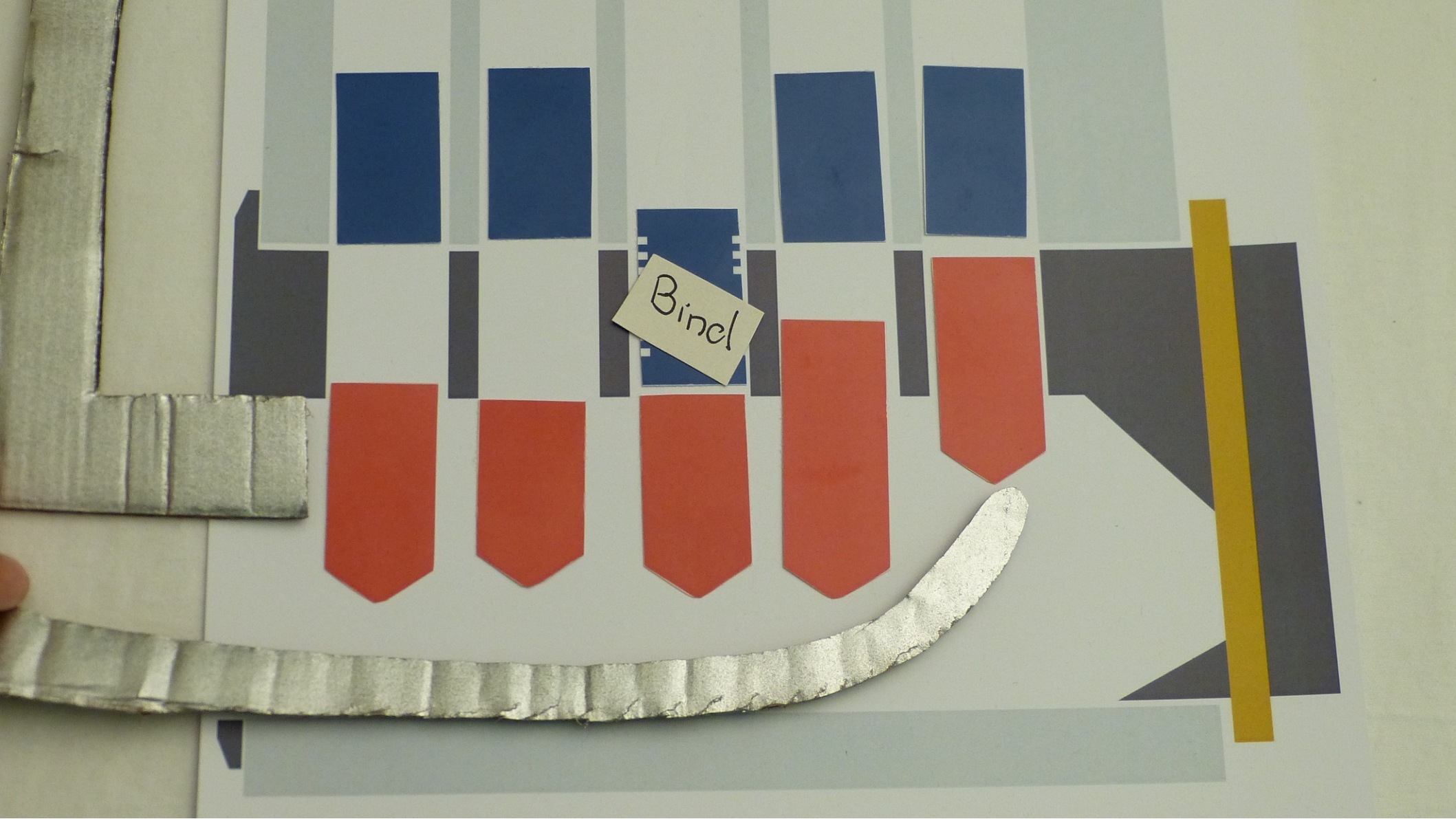


Binel



Binel

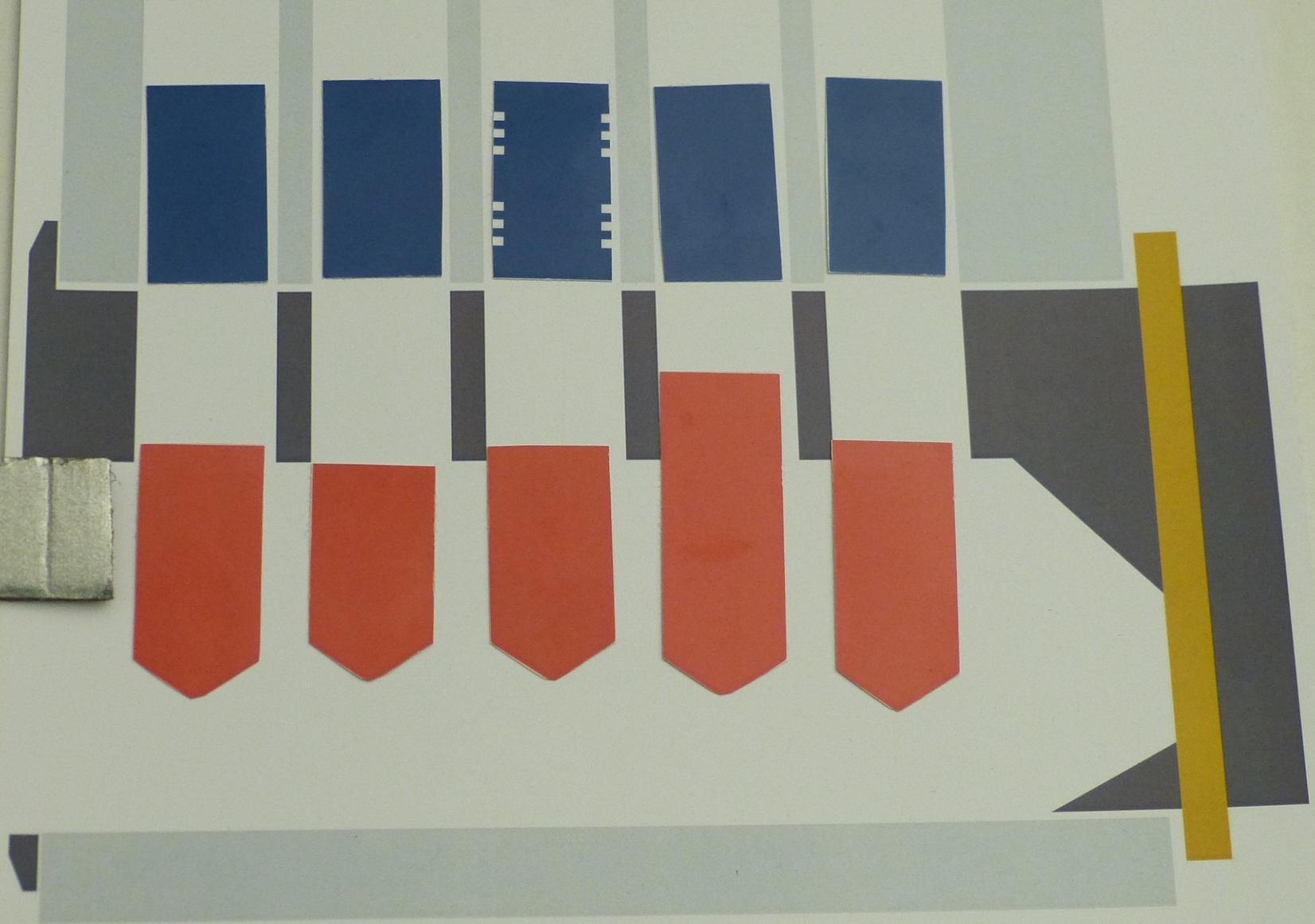
Binel



Bincl

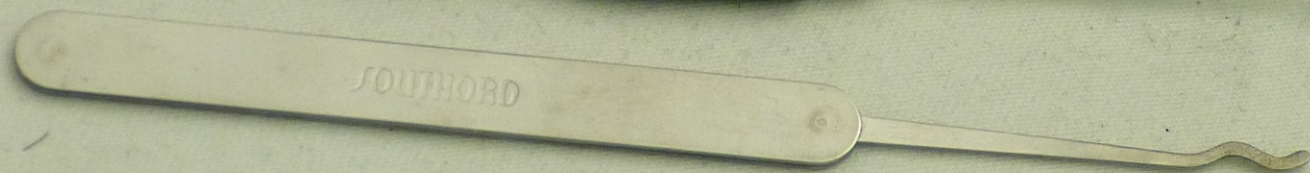
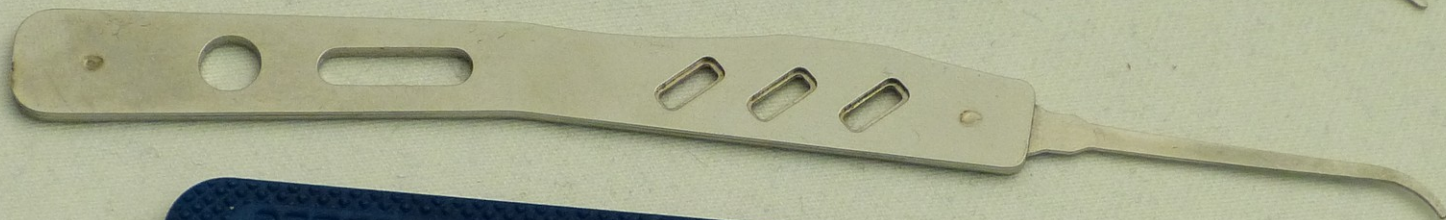
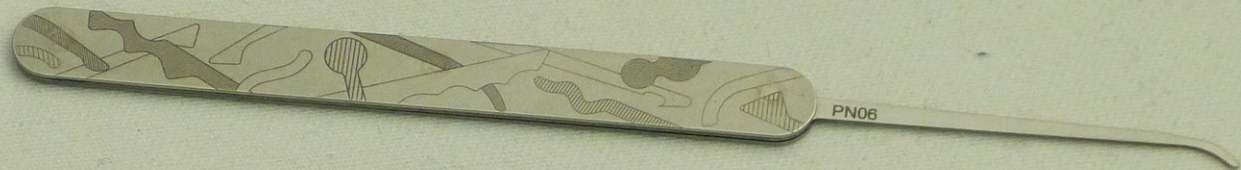


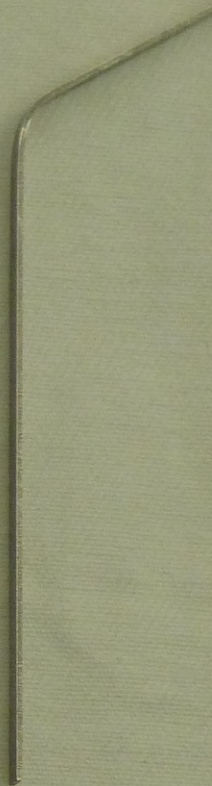
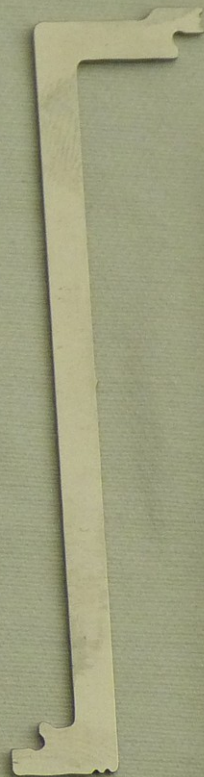
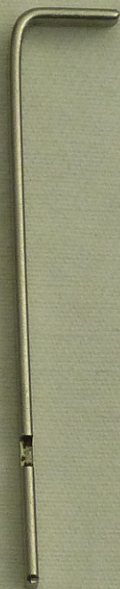
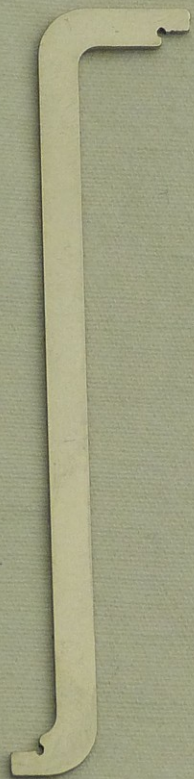
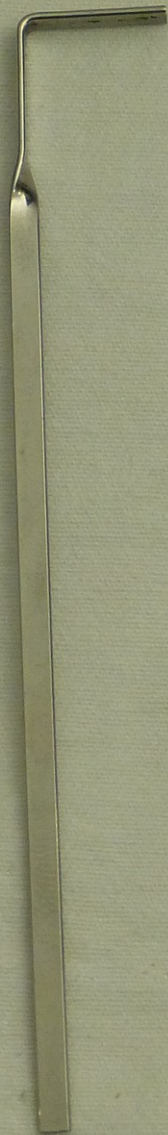
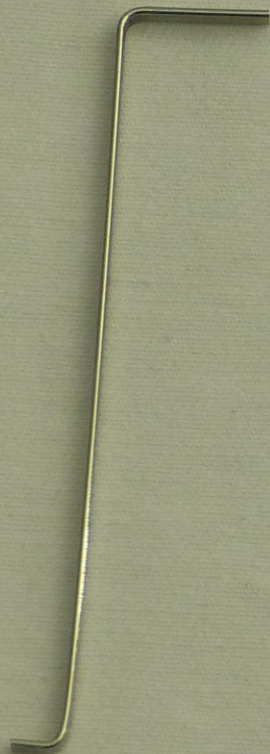
Binel

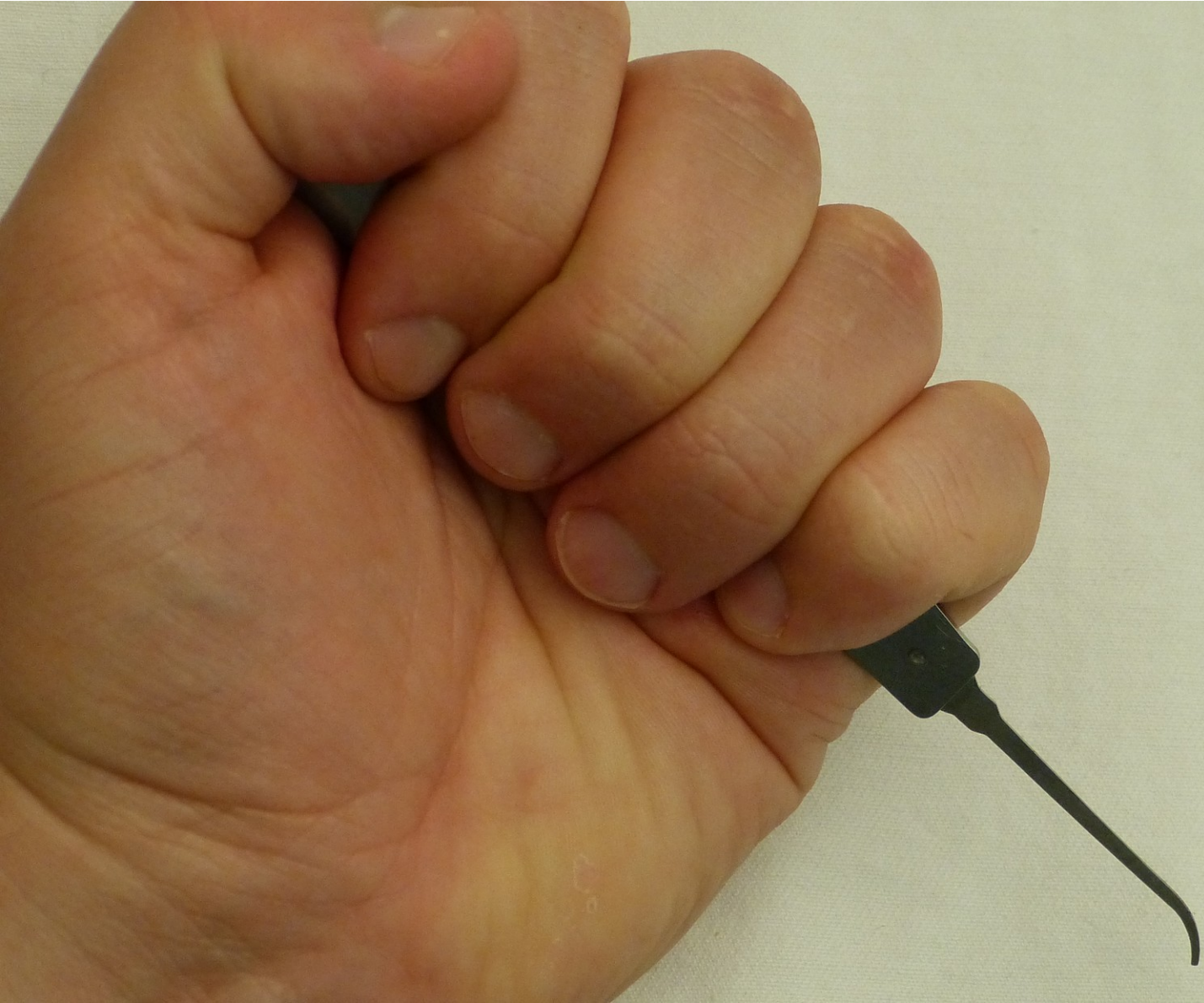


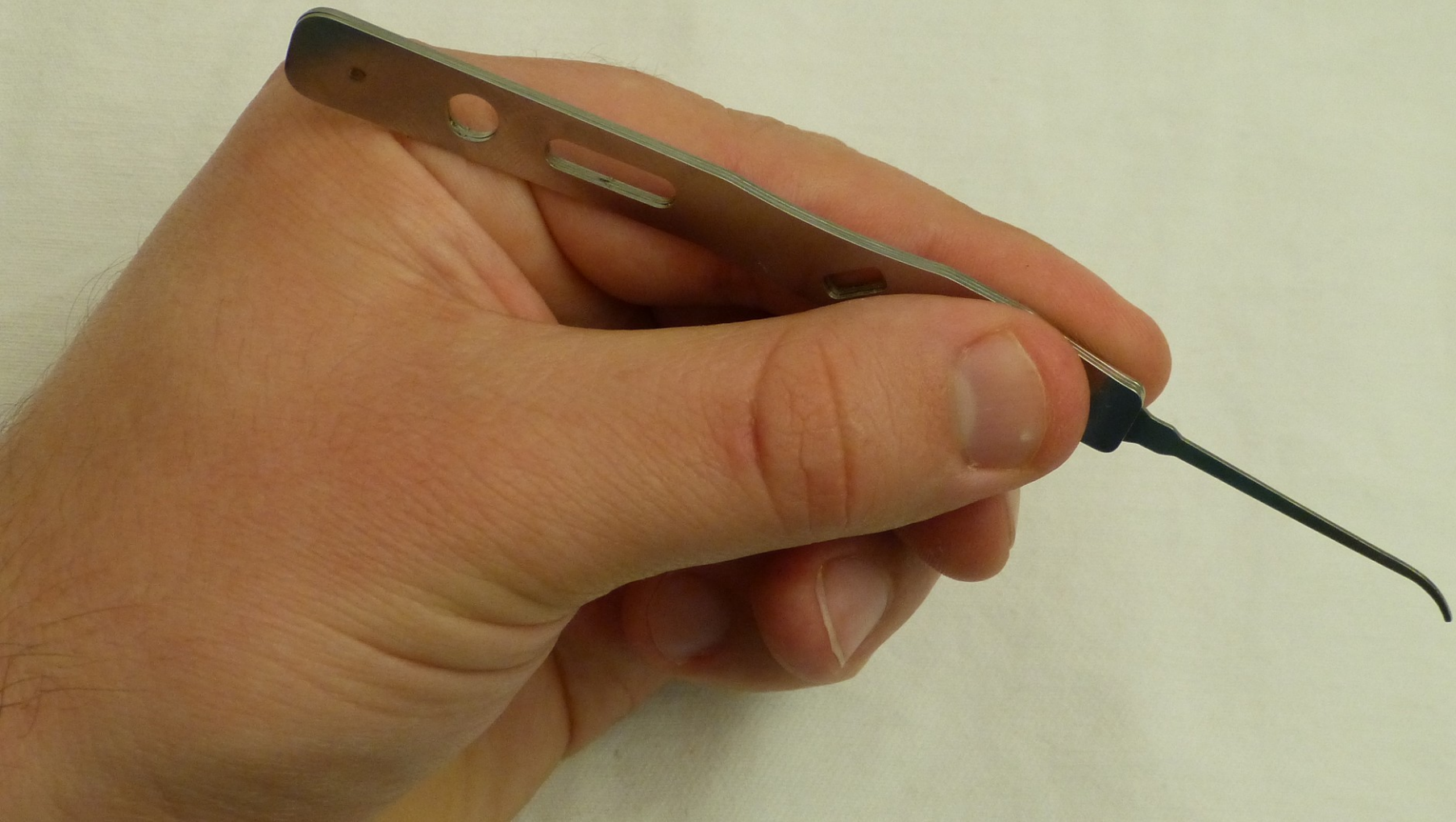


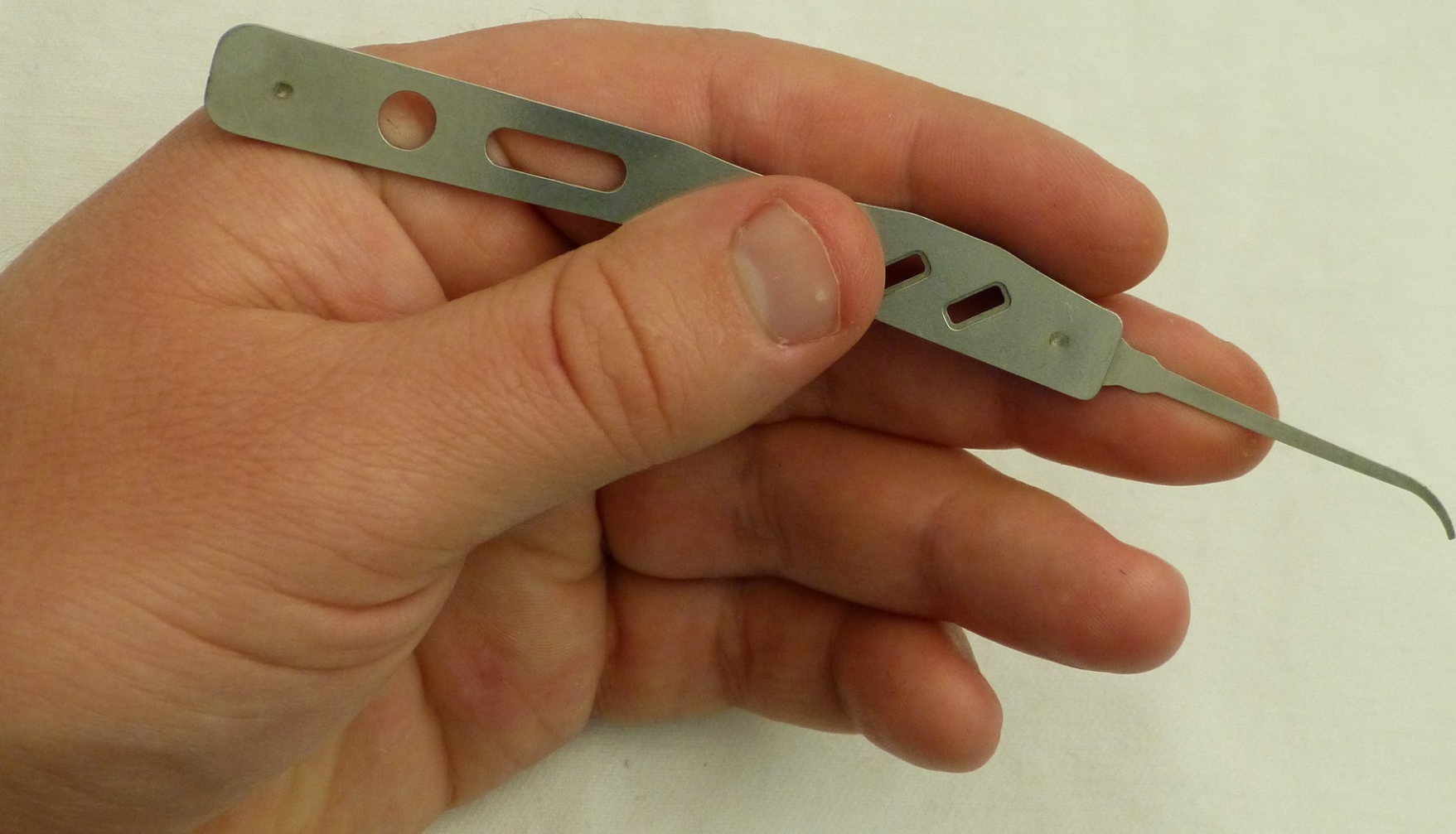


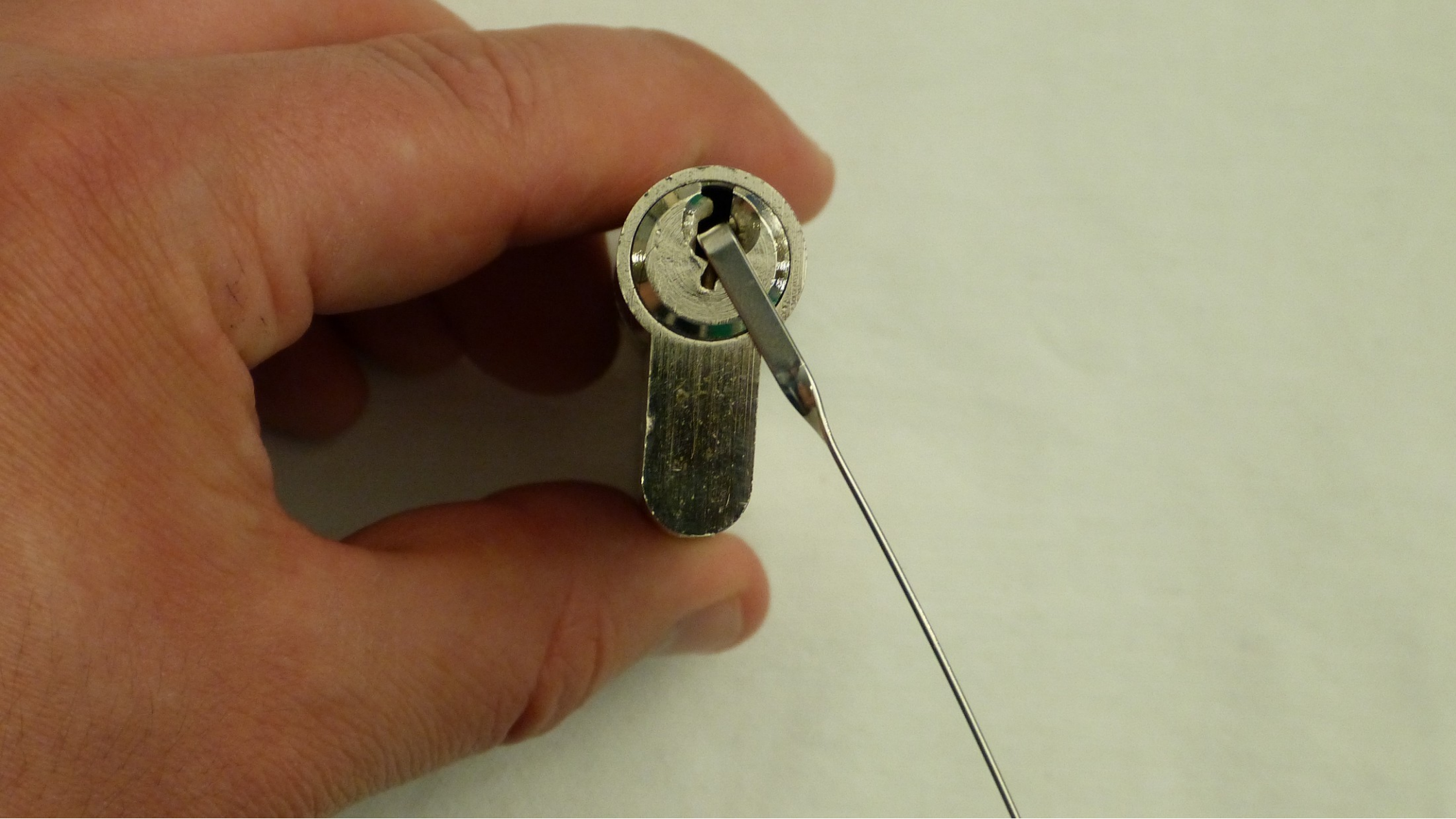


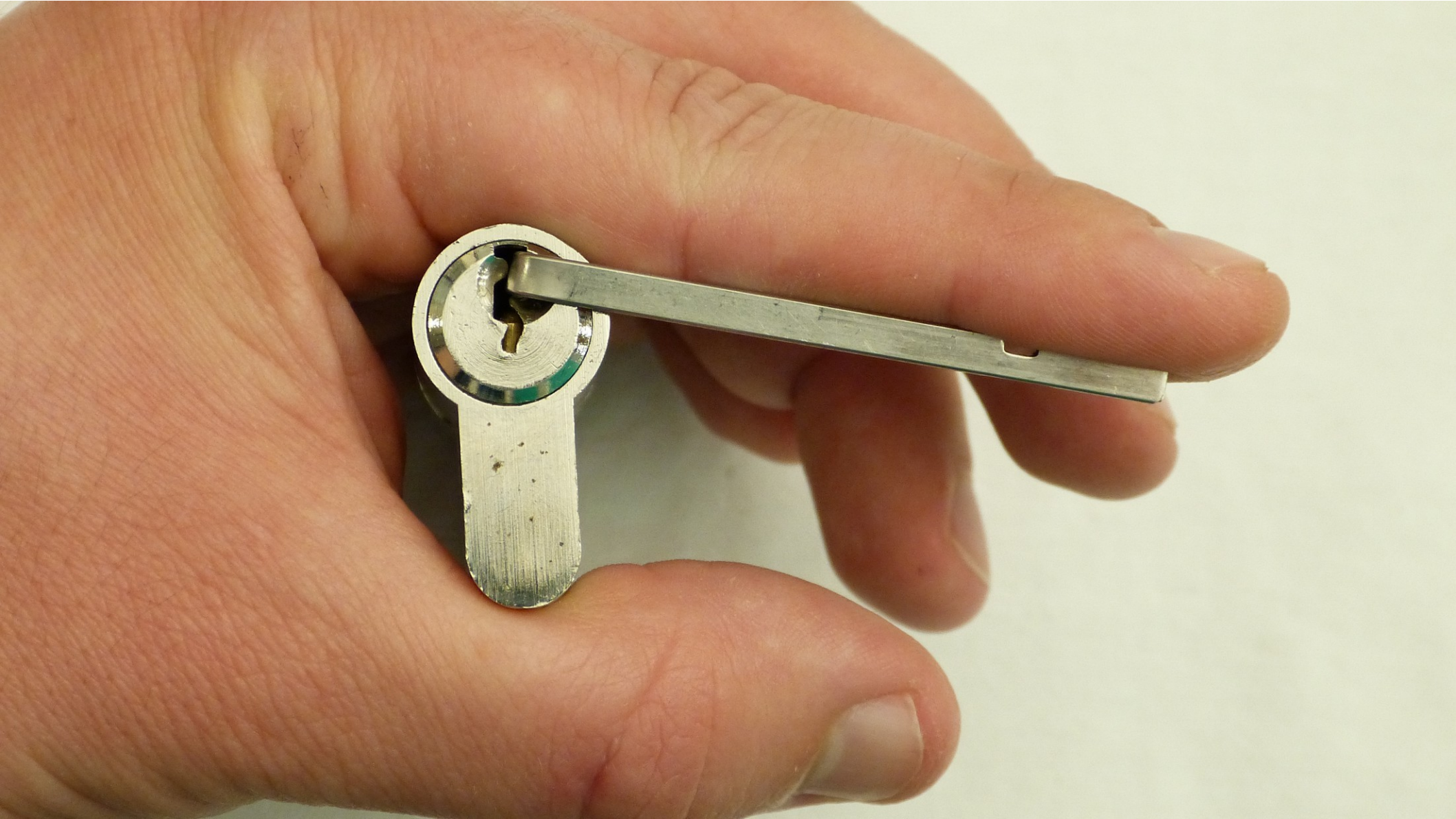


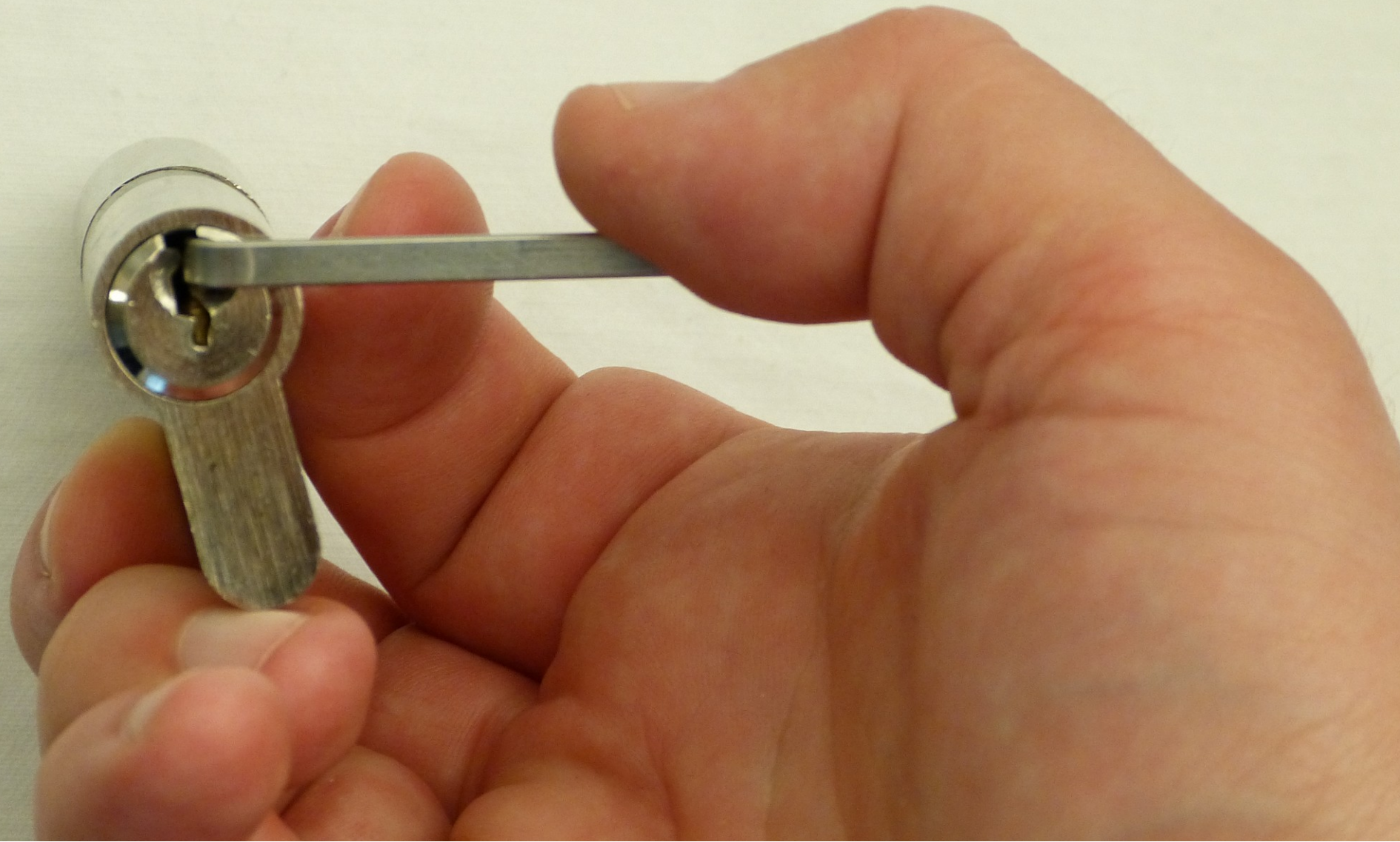








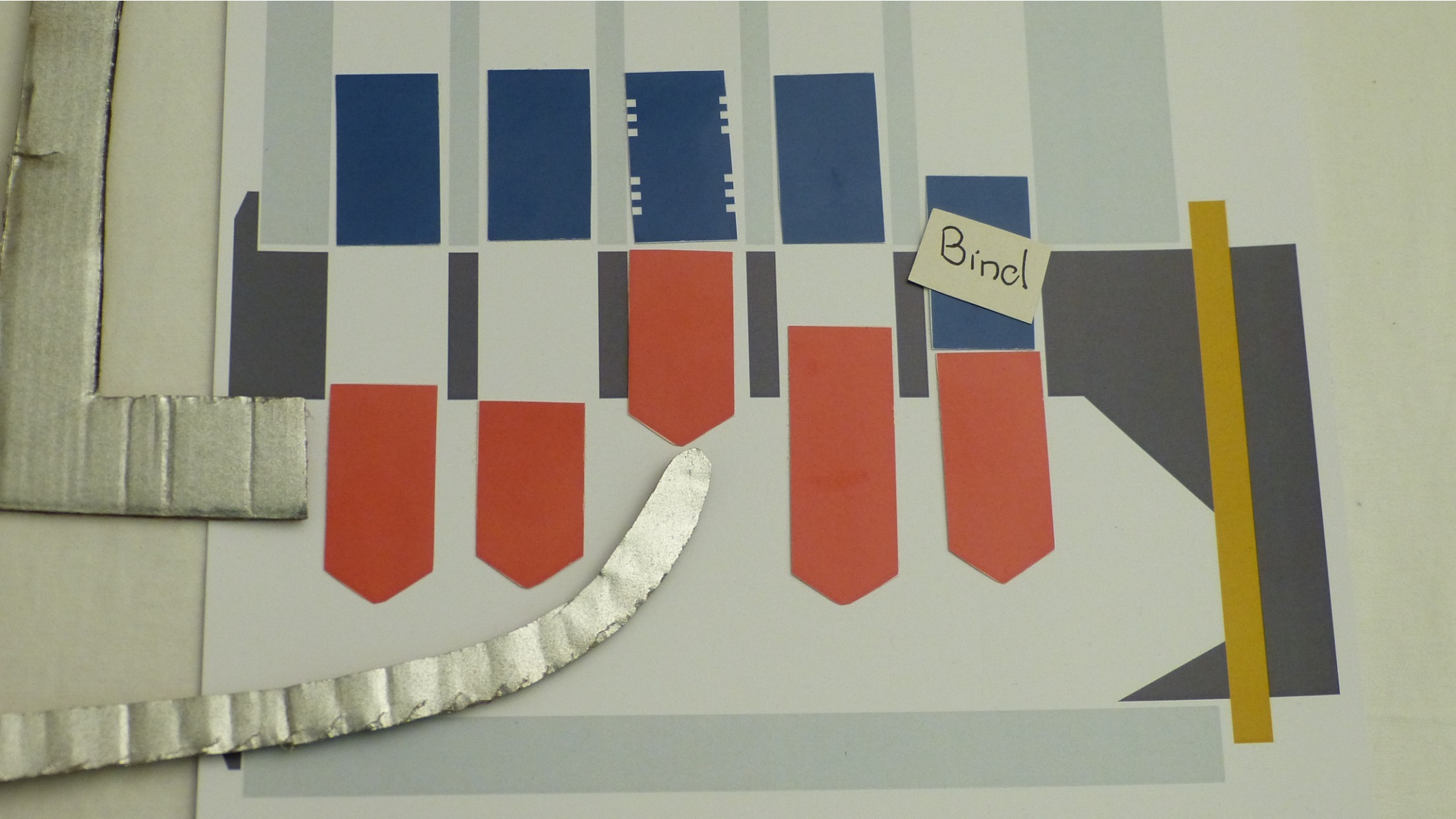




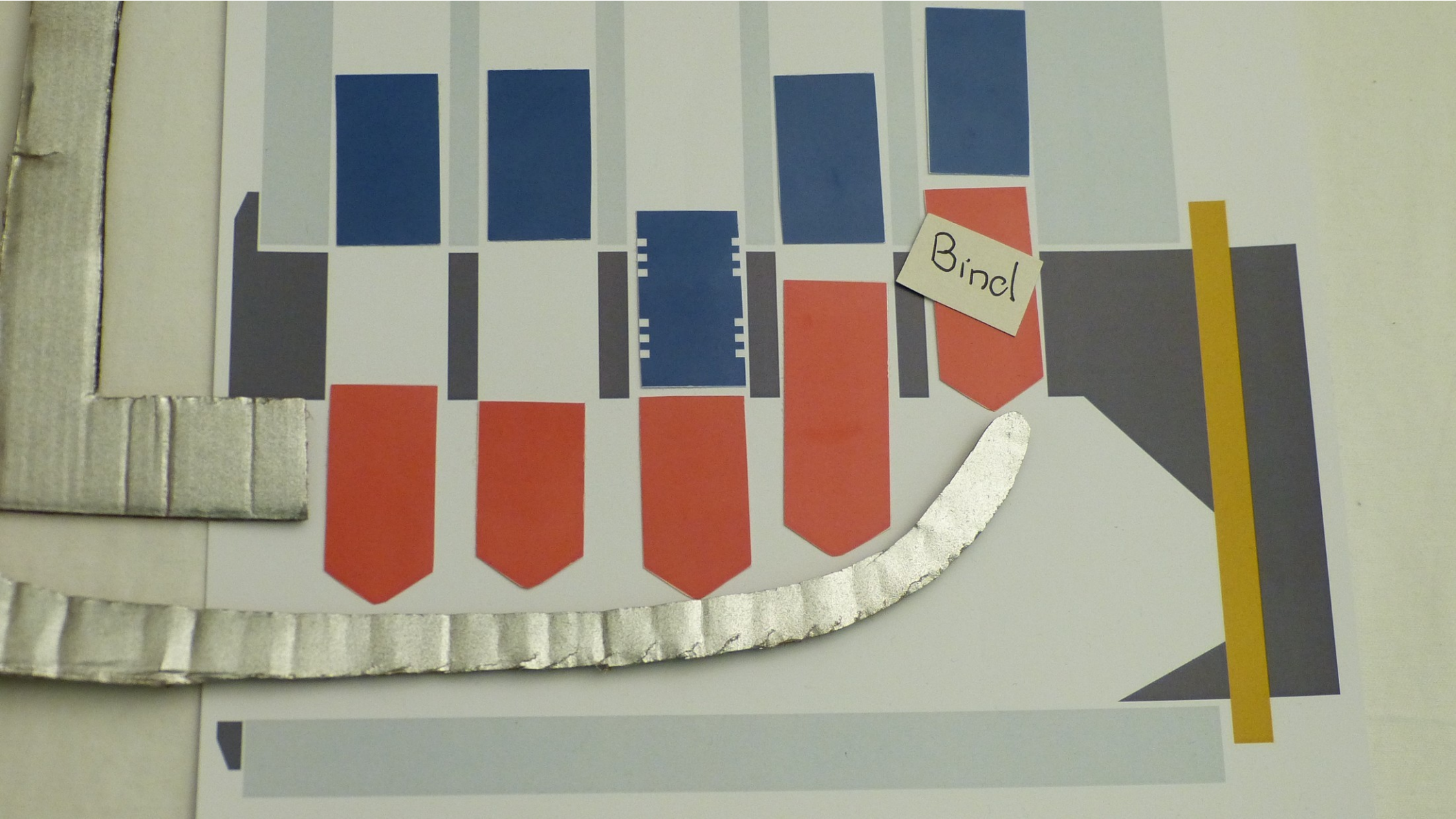
Other pin states

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



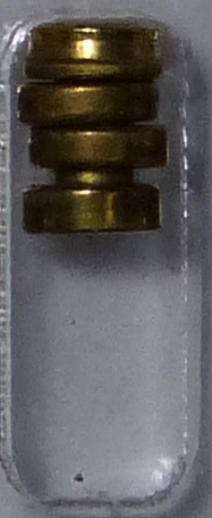


Binel



Binel





Mechanical Safe Lock

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

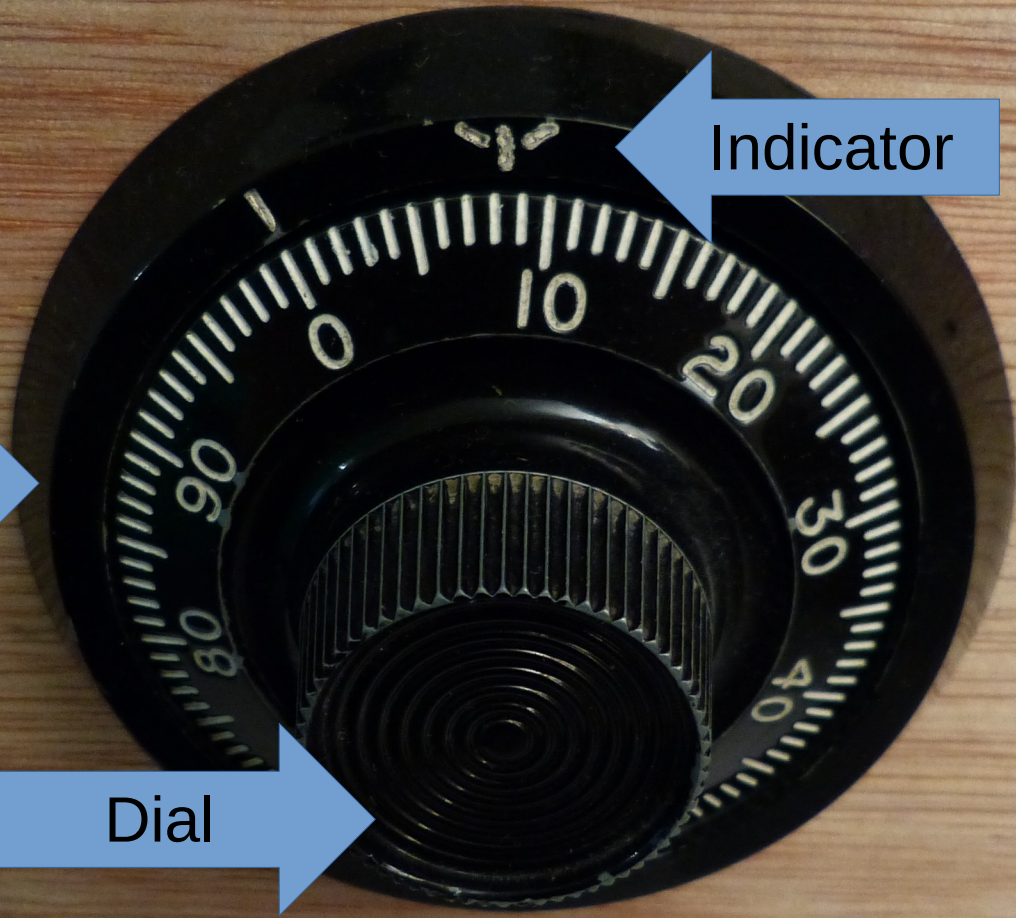
Mechanical Safe Lock

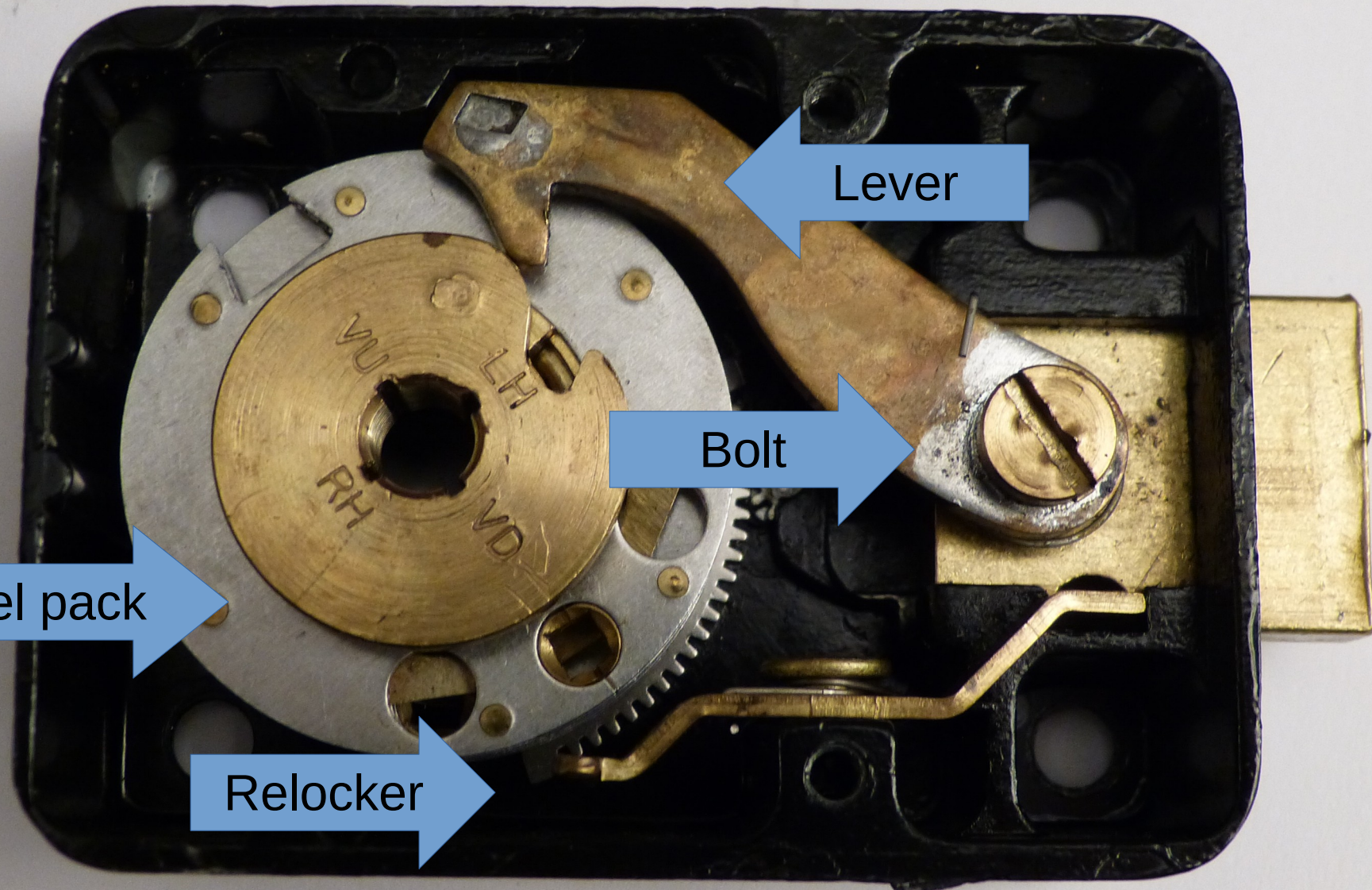
- Target for today:
 - **Sargent Greenleaf 6730**
 - Group 2 safe lock
 - Three wheels
 - Theoretically a million combinations
 - Practically ~400k combinations

Dial ring

Indicator

Dial



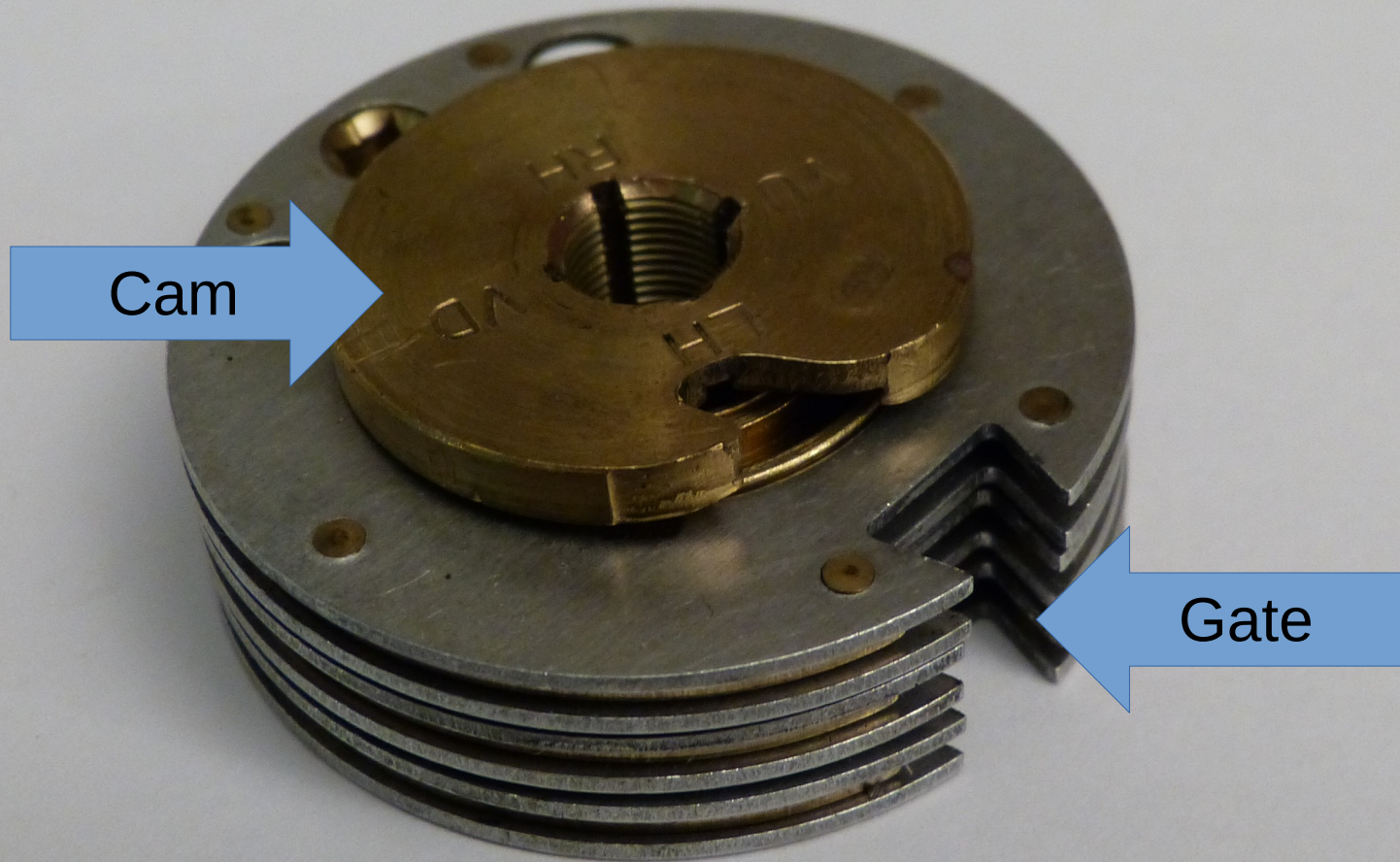


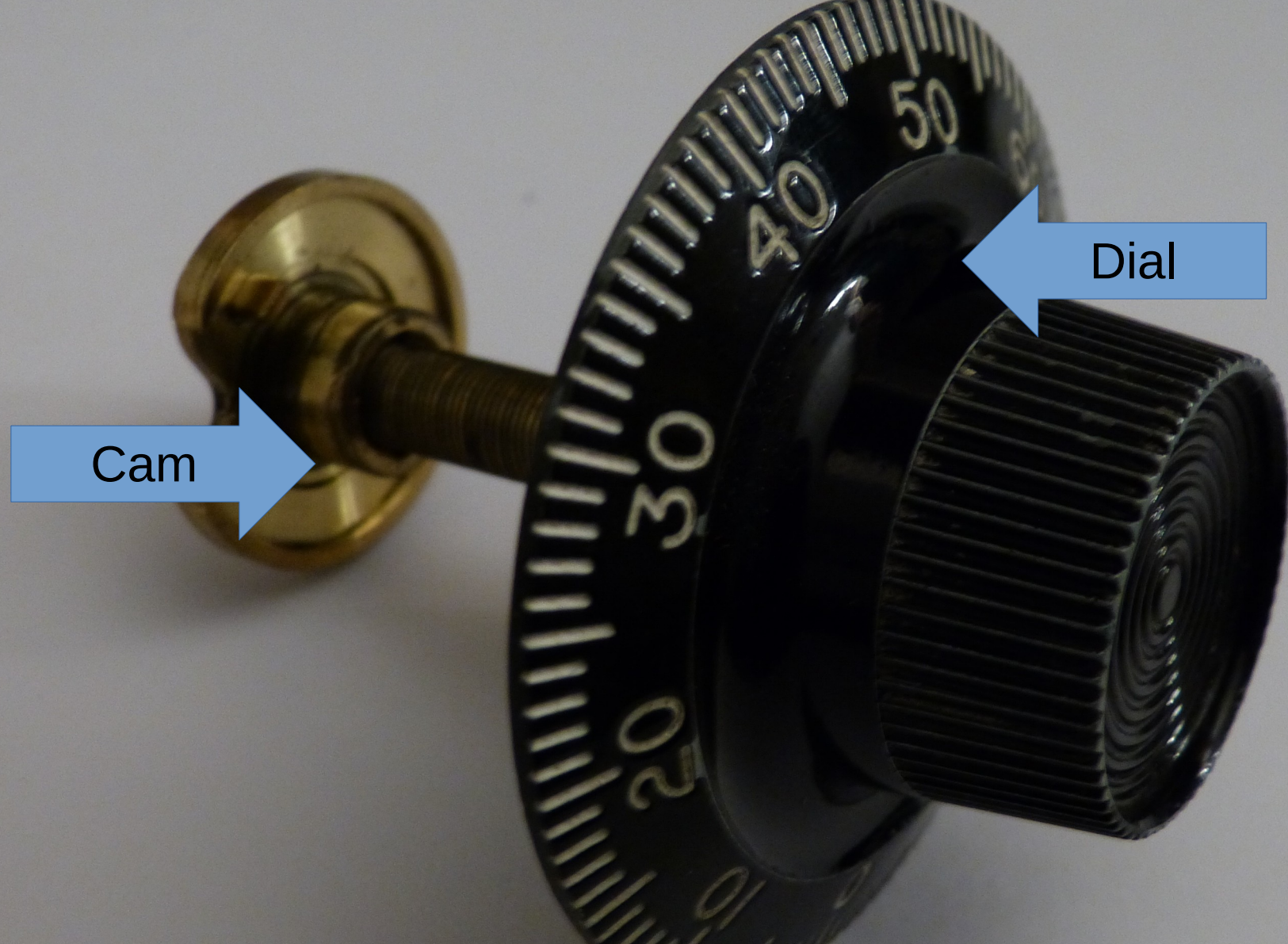
Lever

Bolt

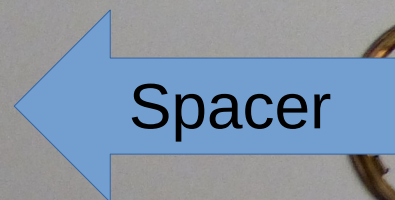
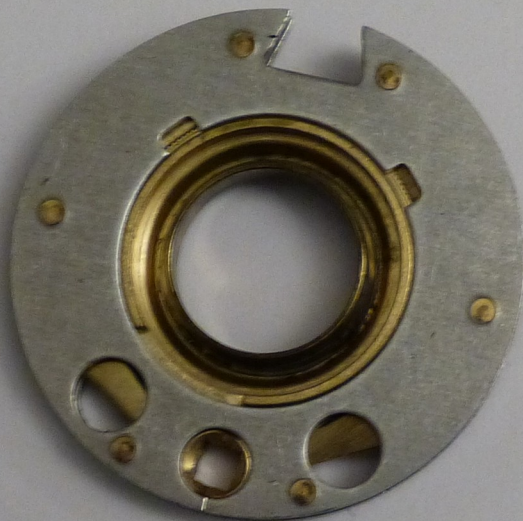
Wheel pack

Relocker









Spacer



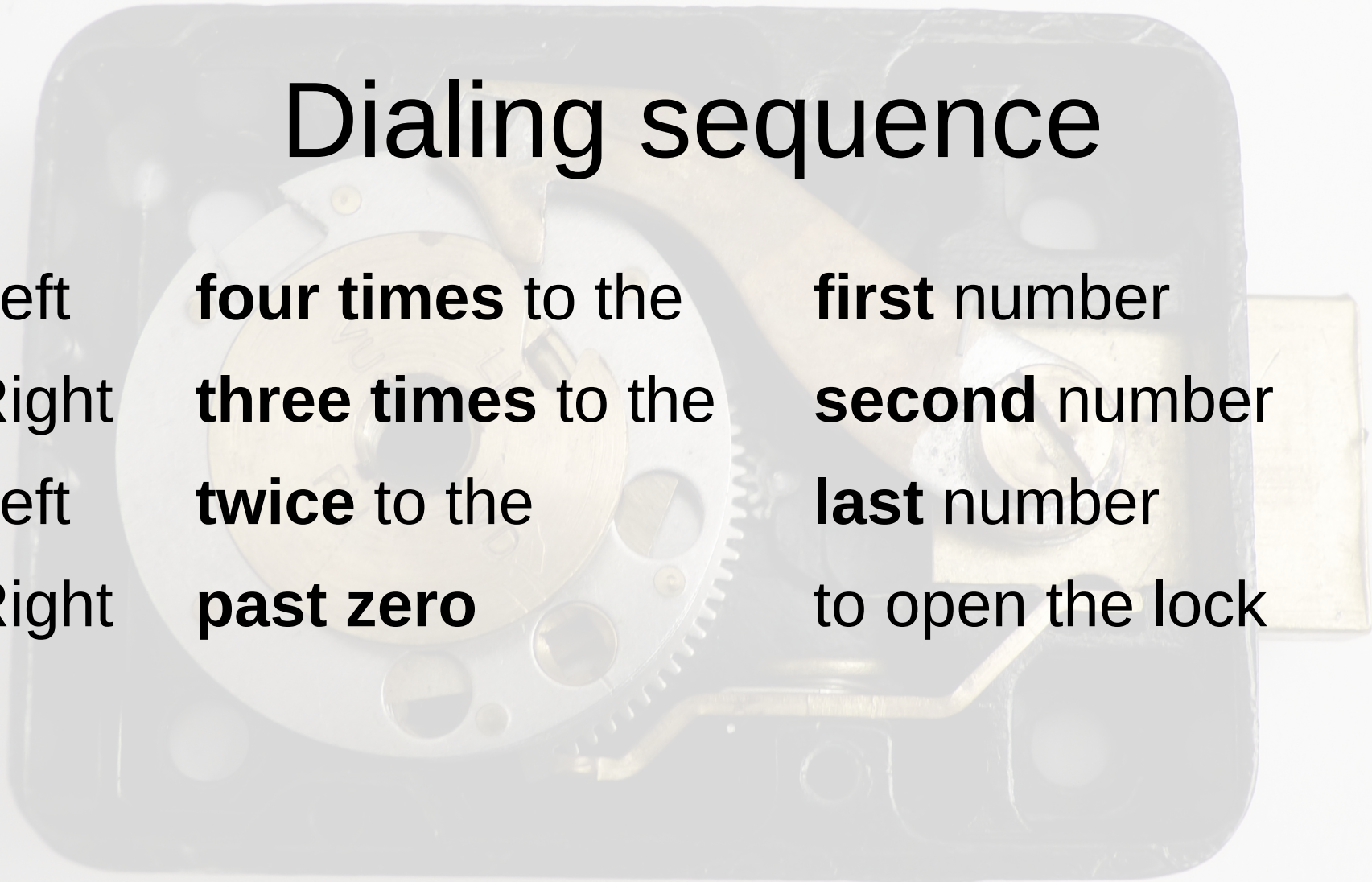
Fly





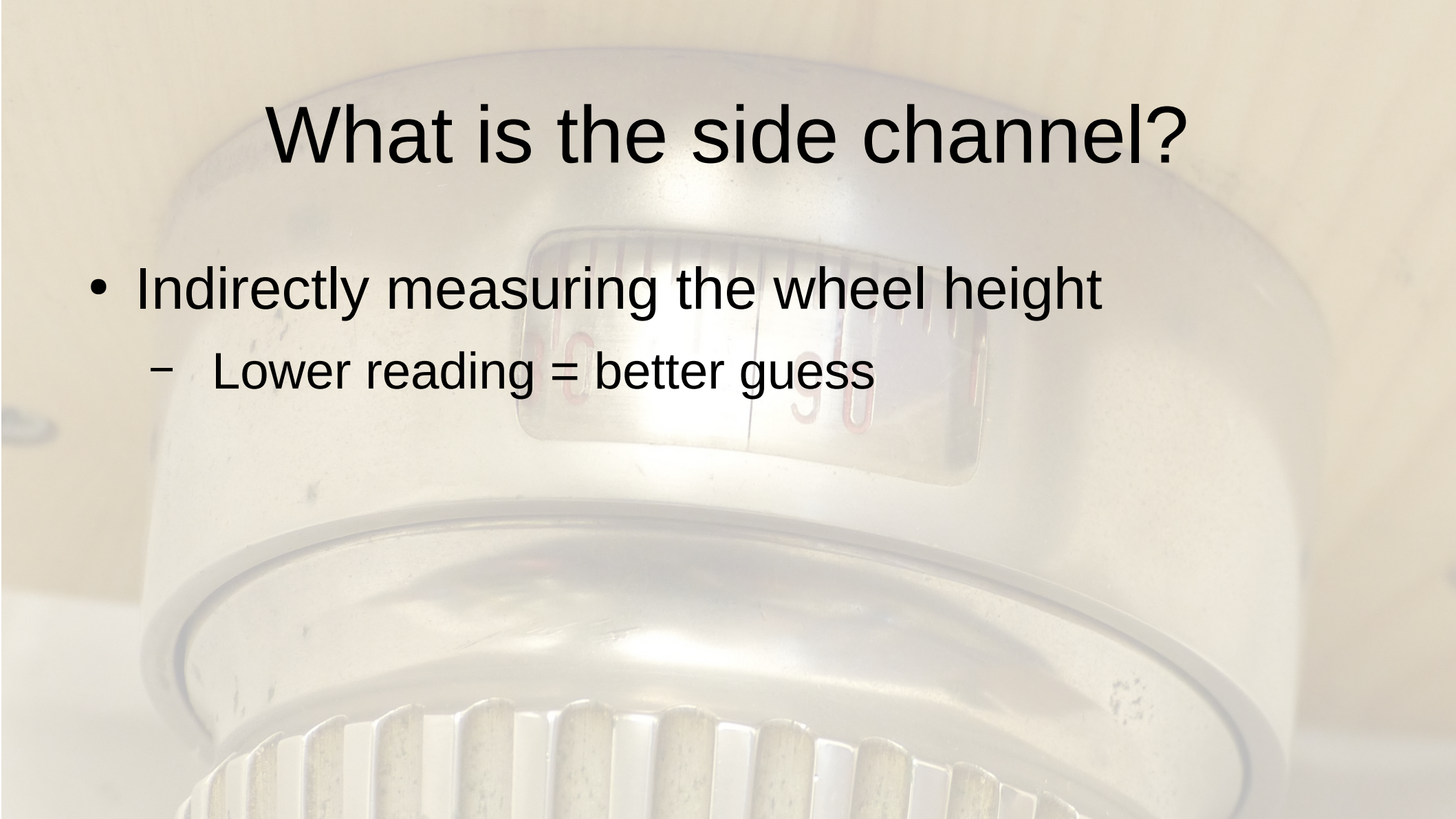


Dialing sequence

- 
- 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

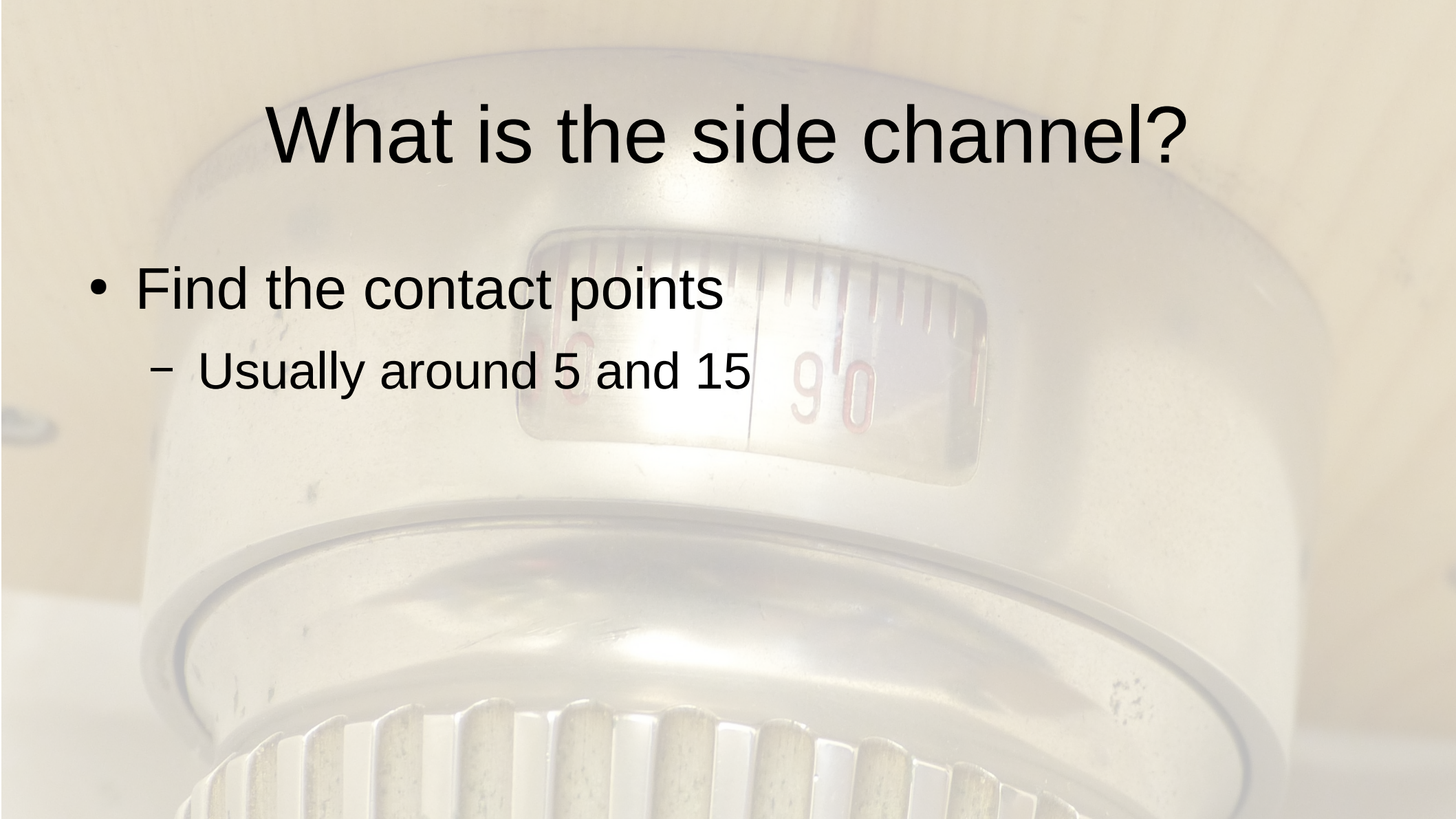
What is the side channel?

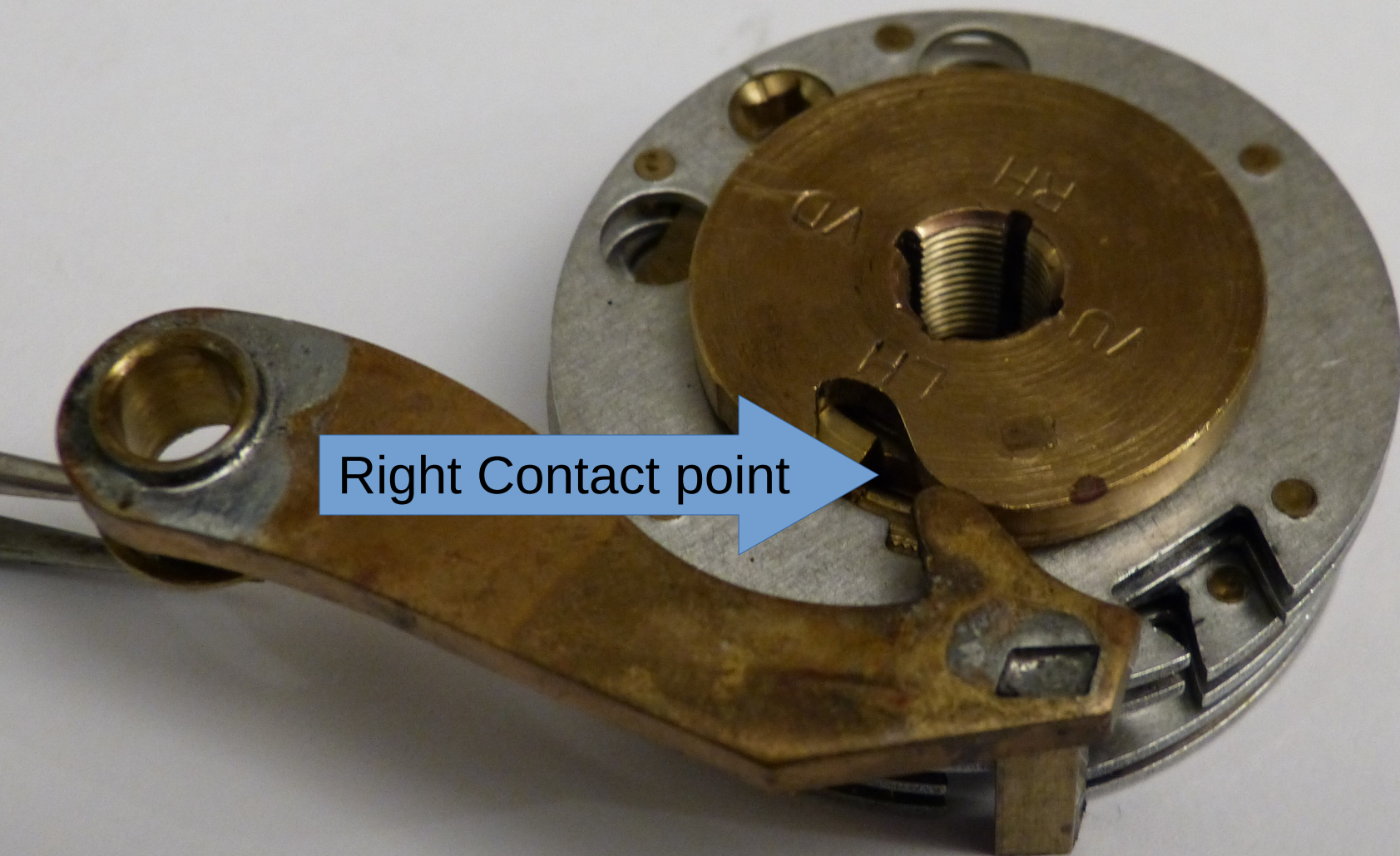
- Indirectly measuring the wheel height
 - Lower reading = better guess



What is the side channel?

- Find the contact points
 - Usually around 5 and 15





Right Contact point



Left Contact point

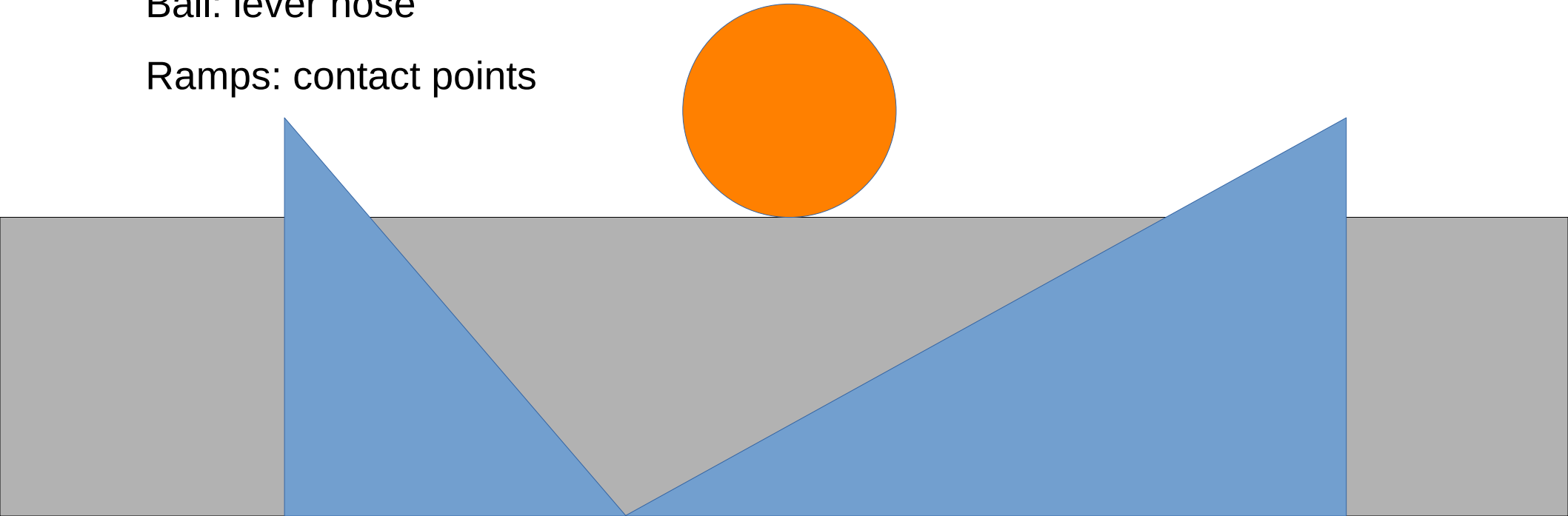
The image shows a mechanical assembly. A circular silver-colored metal plate has a central brass disk. The brass disk has a central threaded hole with a black pin. Engraved on the brass disk are the letters 'RH' at the top, 'VD' on the left, and 'LH' at the bottom. A blue arrow points from the text 'Left Contact point' to a contact point on the brass disk. To the left of the brass disk is a curved brass arm with a circular hole at its end. The entire assembly is set against a white background.

Manipulation process

Gray: Wheel

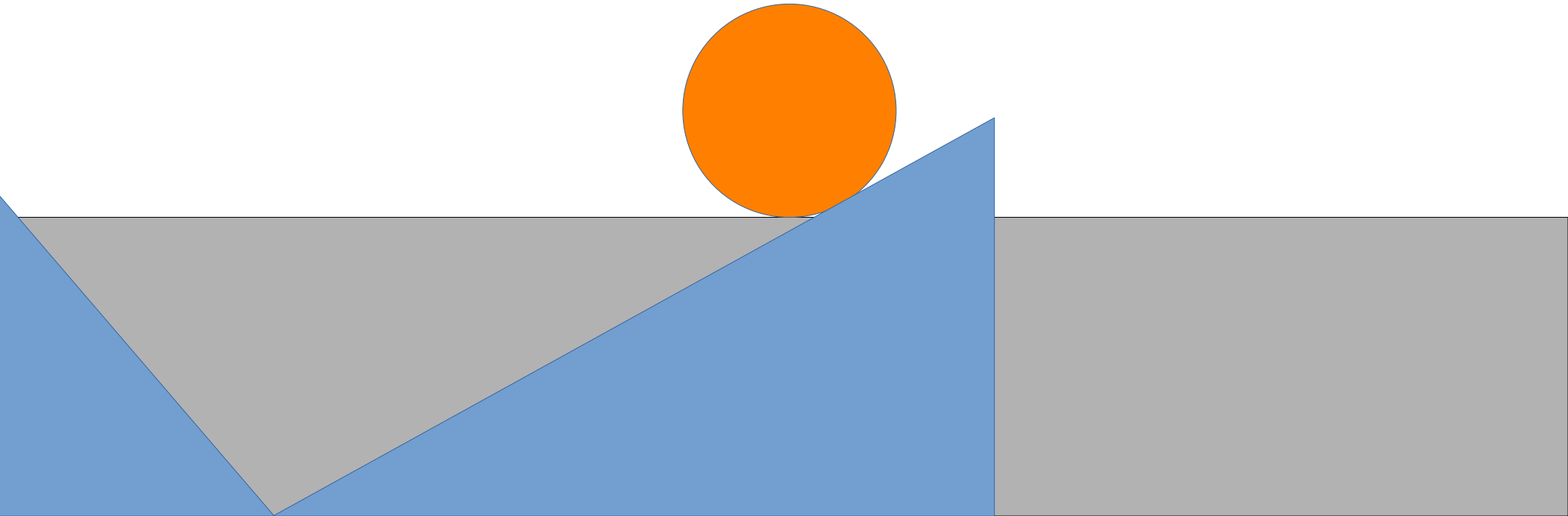
Ball: lever nose

Ramps: contact points



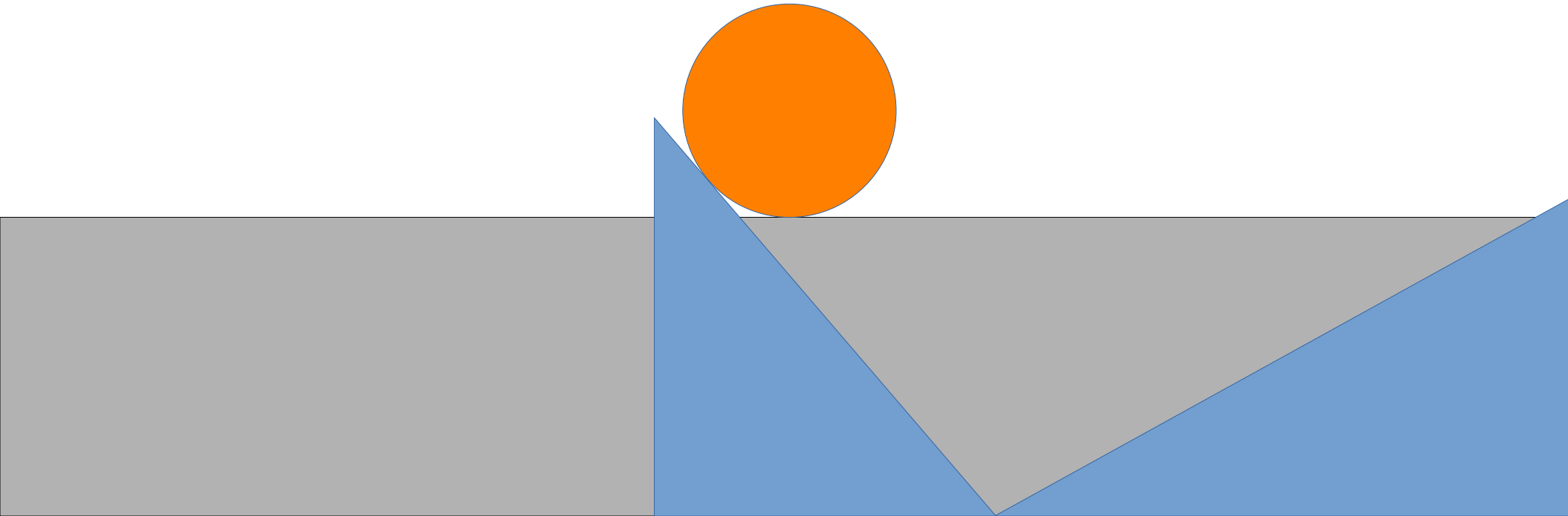
Manipulation process

Right contact point

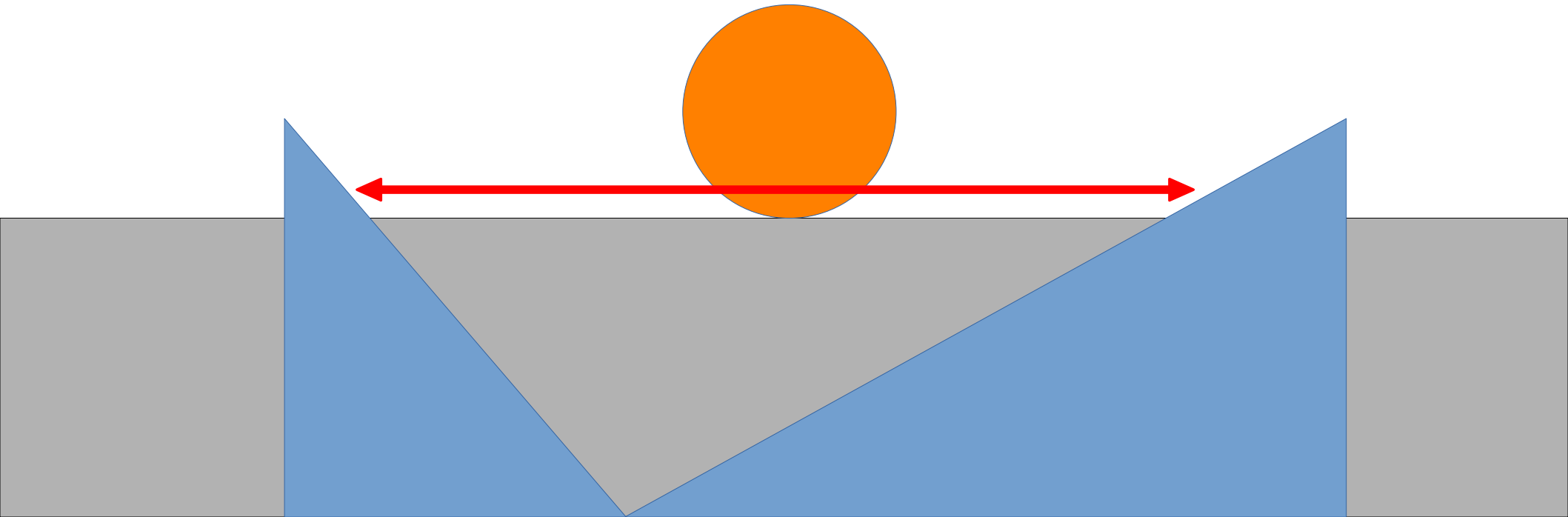


Manipulation process

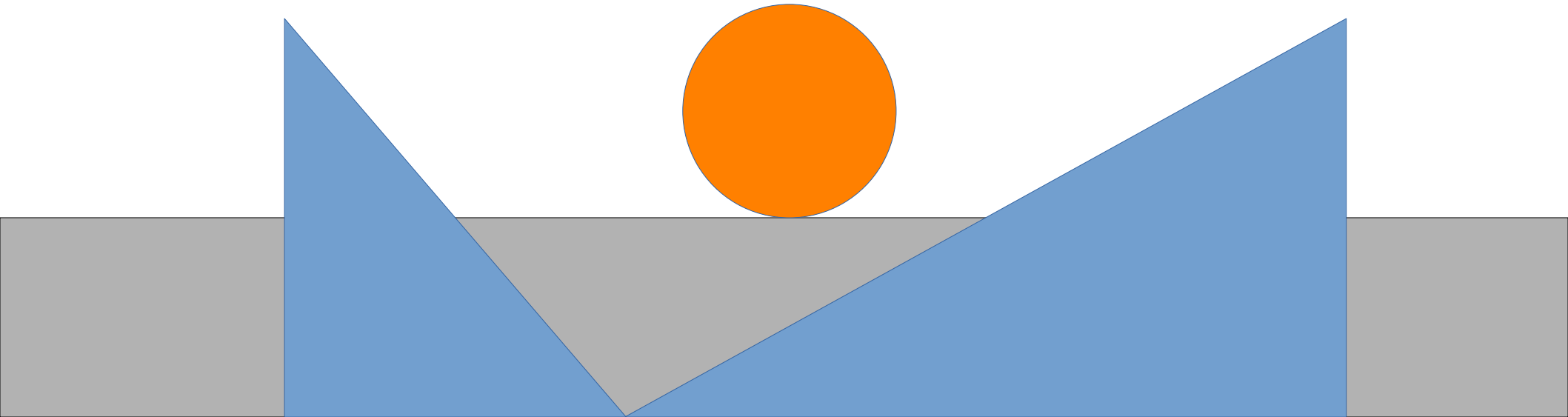
Left contact point



Manipulation process

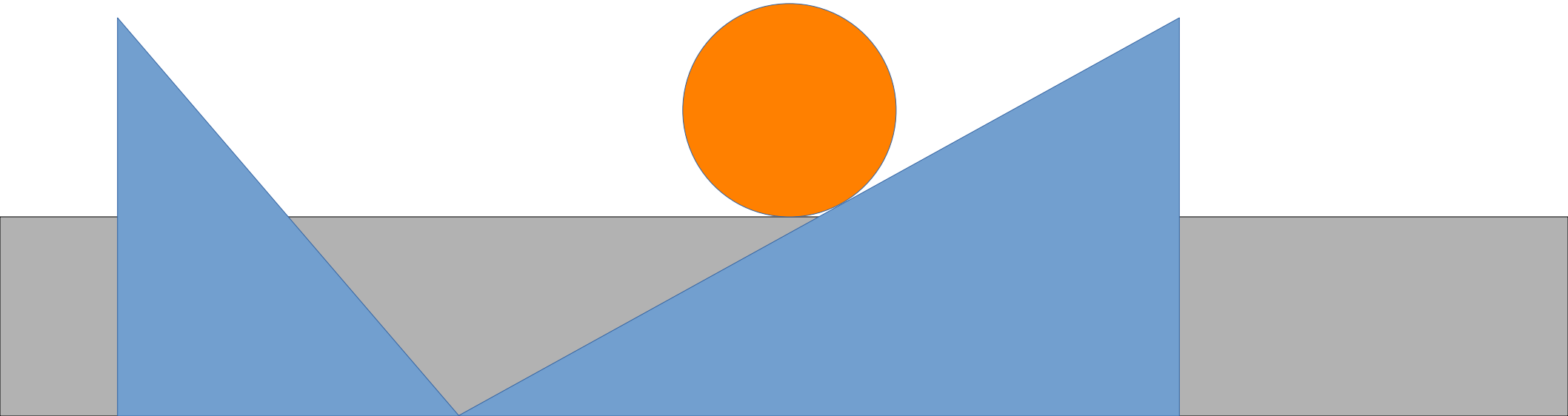


Manipulation process



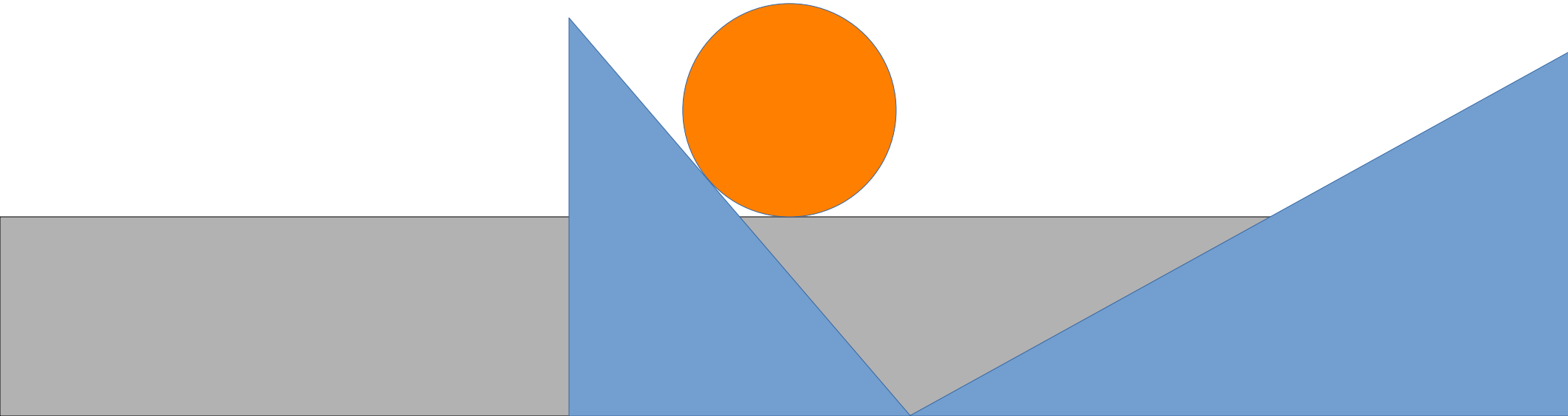
Manipulation process

Right contact point

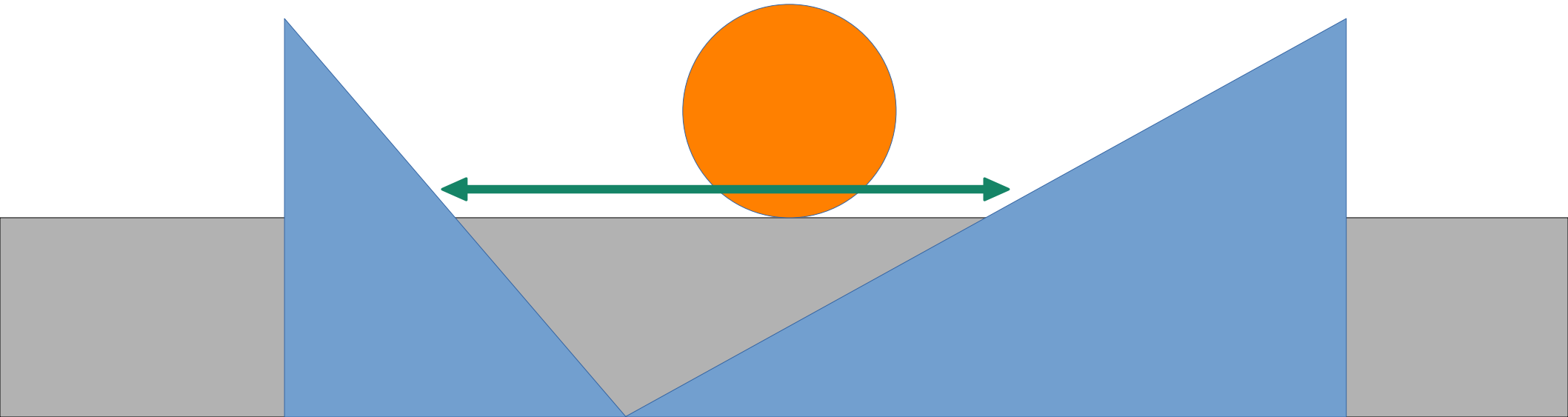


Manipulation process

Left contact point

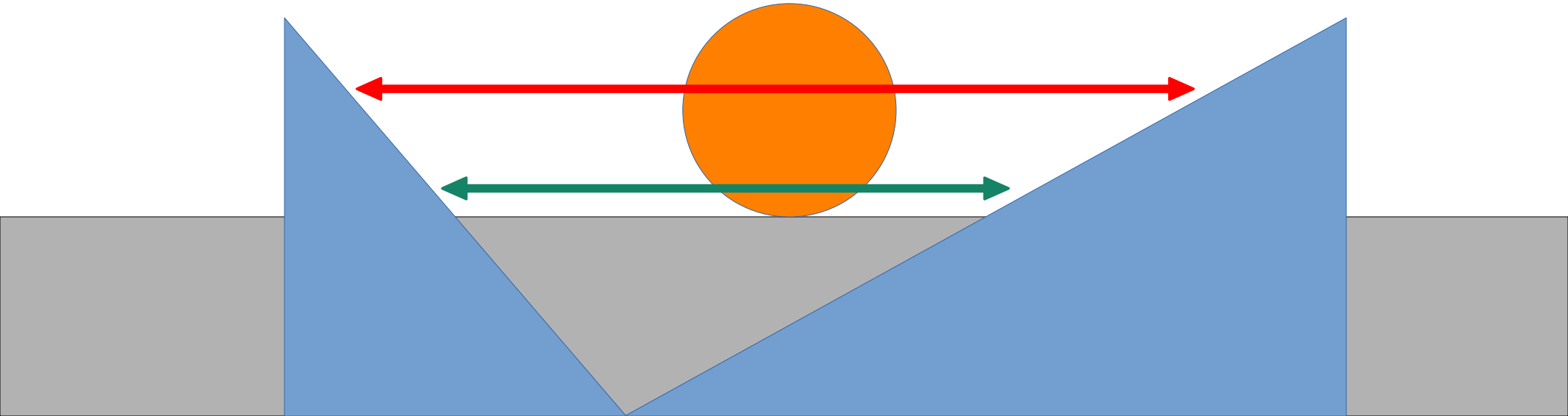


Manipulation process



Manipulation process

Shorter distance = more correct





No gate

The image shows a close-up of a mechanical assembly. At the top, a brass-colored component is visible, with a blue arrow pointing to it from the right. Below this, a black semi-circular scale is mounted on a white plastic base. The scale has white markings and numbers: 0, 10, 20, and 30. The scale is positioned such that the 0 mark is on the left and the 30 mark is on the right. The white plastic base has two small circular holes on the left side.



No gate

Value 13.25



Gate of wheel 3

A close-up photograph of a mechanical dial, likely from a cryptographic device. The dial is black with white markings. It features a scale from 0 to 30, with major numbers at 0, 10, 20, and 30. Between these major numbers are ten smaller tick marks, indicating increments of 2. A white pointer is visible at the top of the dial, pointing to the 10 mark. The dial is mounted on a light-colored, possibly white, plastic or metal base. In the background, some mechanical components, including a brass-colored spring, are visible. A blue arrow points from the text 'Gate of wheel 3' to the dial.



Wheel 3 gate

The image shows a close-up of a mechanical device. At the top, there is a brass-colored component with a series of thin, curved blades or gates. A blue arrow points from the text 'Wheel 3 gate' to this component. Below this, there is a black, semi-circular scale with white markings. The scale has major numbers at 0, 10, 20, and 30, and minor markings every 1 unit. A blue arrow points from the text 'Value 13.00' to the 13th mark on the scale. The device is mounted on a light-colored, possibly white, plastic or metal base.

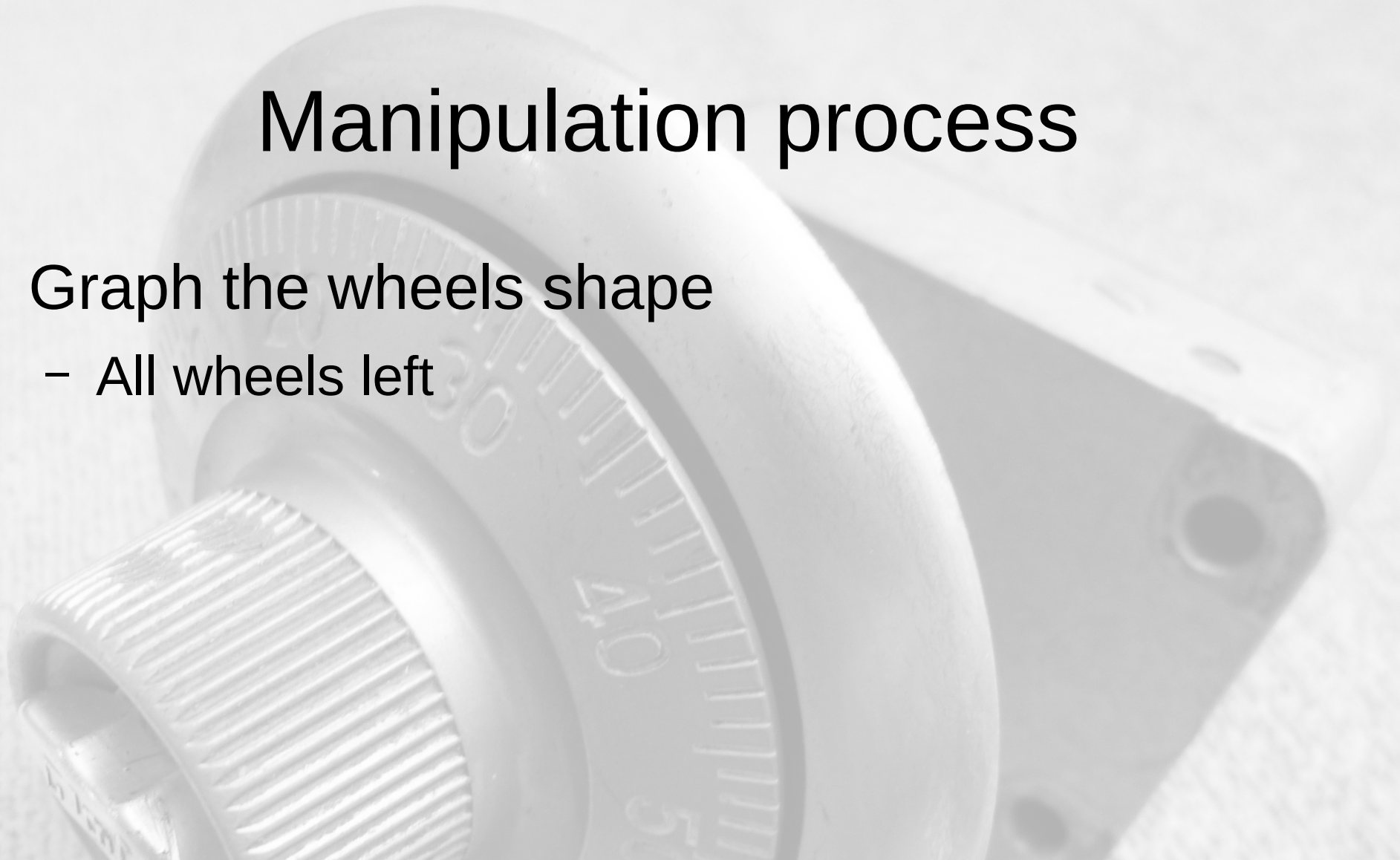
Value 13.00

Manipulation process

- Measuring precision
 - Traditionally $\frac{1}{8}$ th of a digit
 - 0.1 increments work as well

Manipulation process

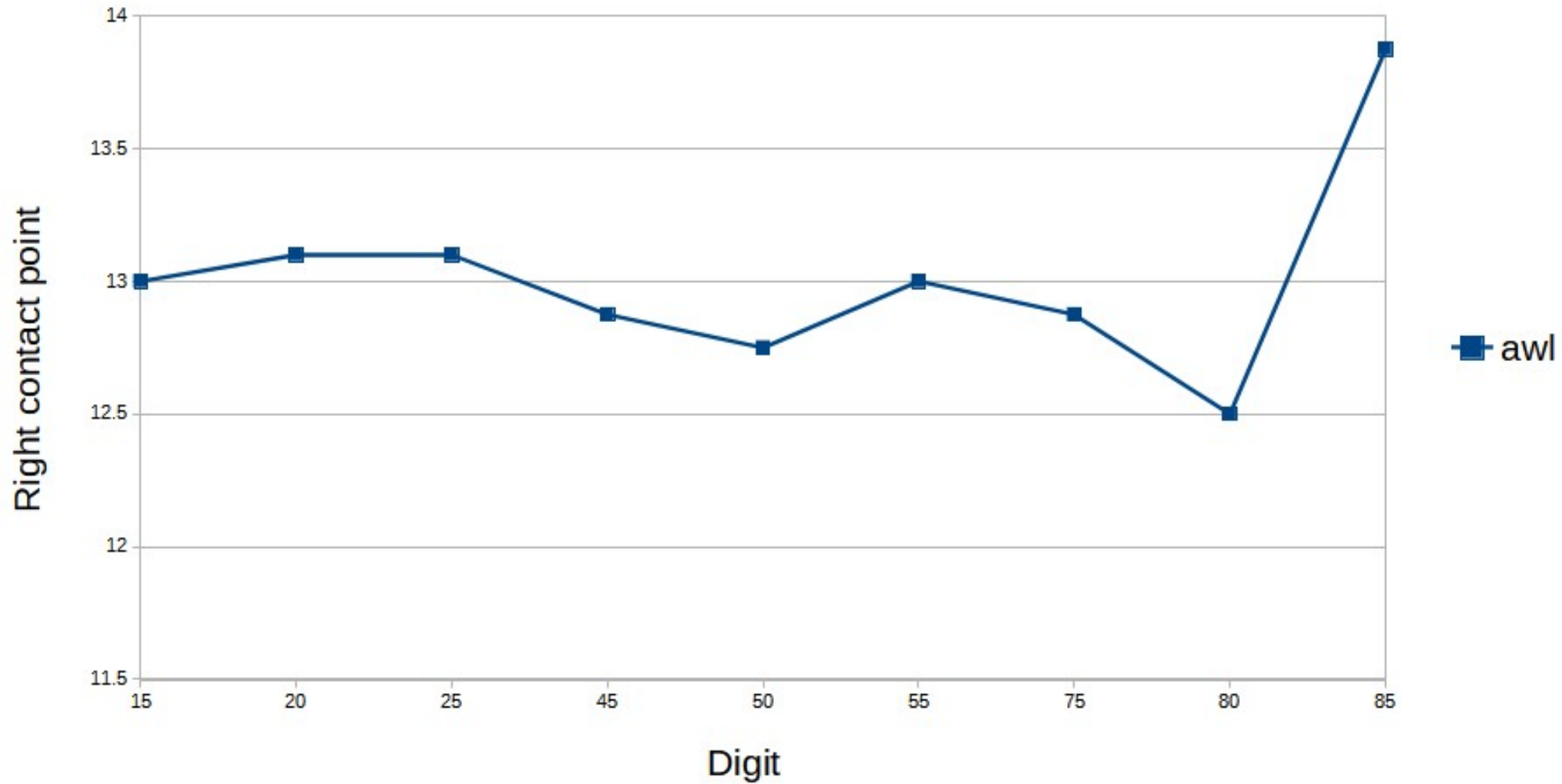
- Graph the wheels shape
 - All wheels left



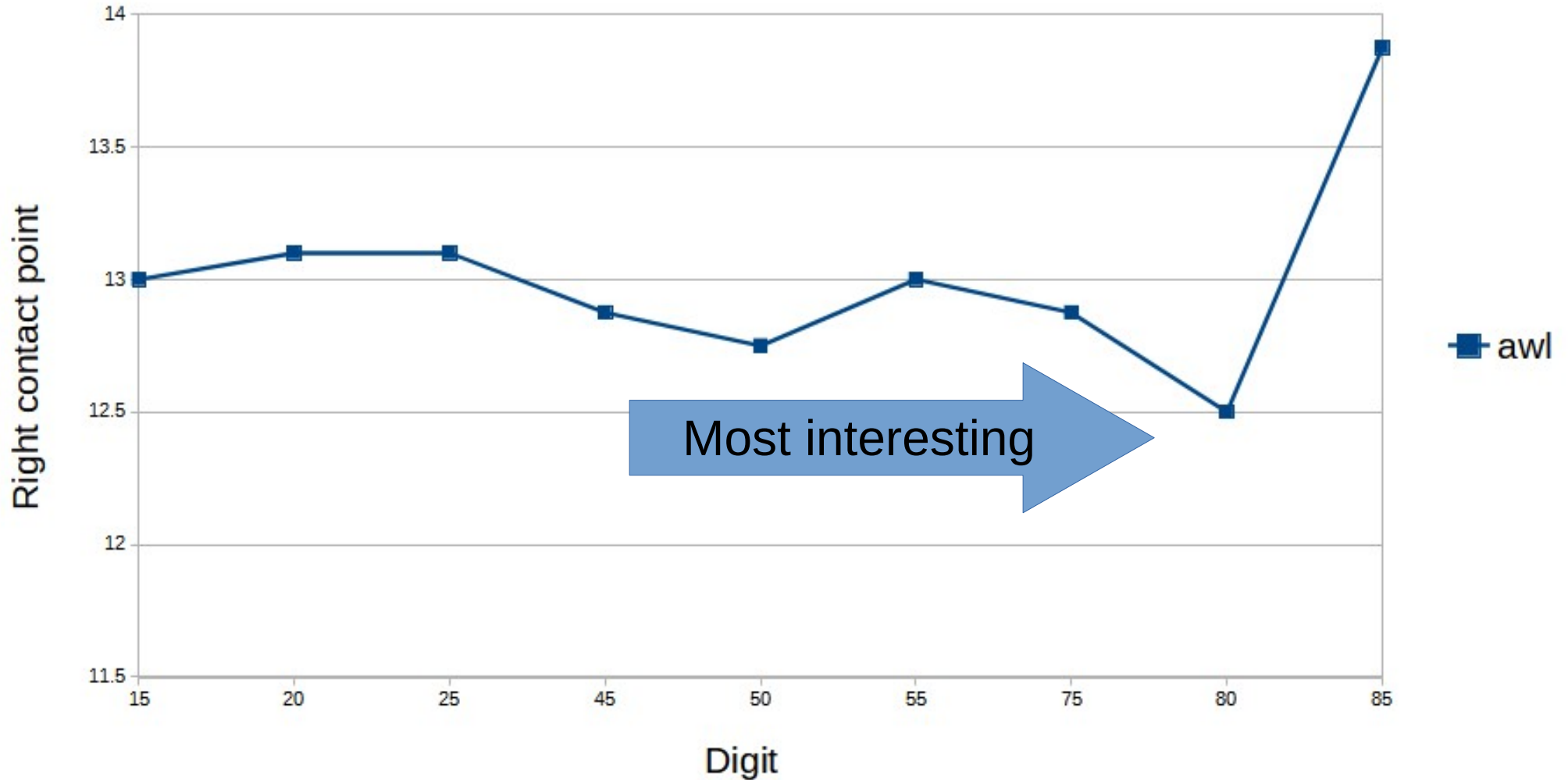
Manipulation process

- 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



First graph: S&G 6730



Manipulation process

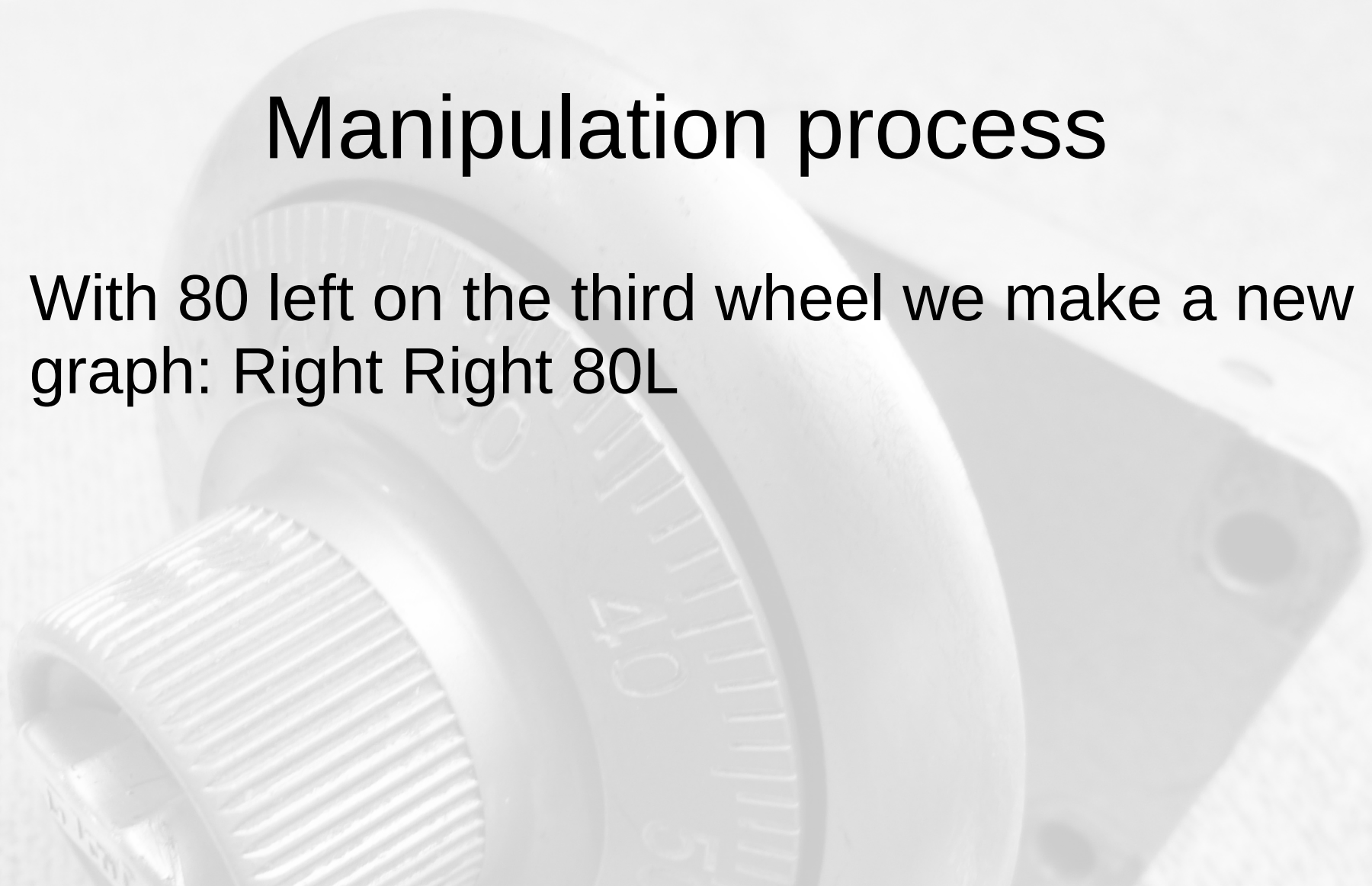
- We need to test which wheel is the lowest point is
 - We dial:
 - 80L 80L 70R and take a reading
 - 70R 80L 80L and take a reading
 - 80L 70R 80L and take a reading

Manipulation process

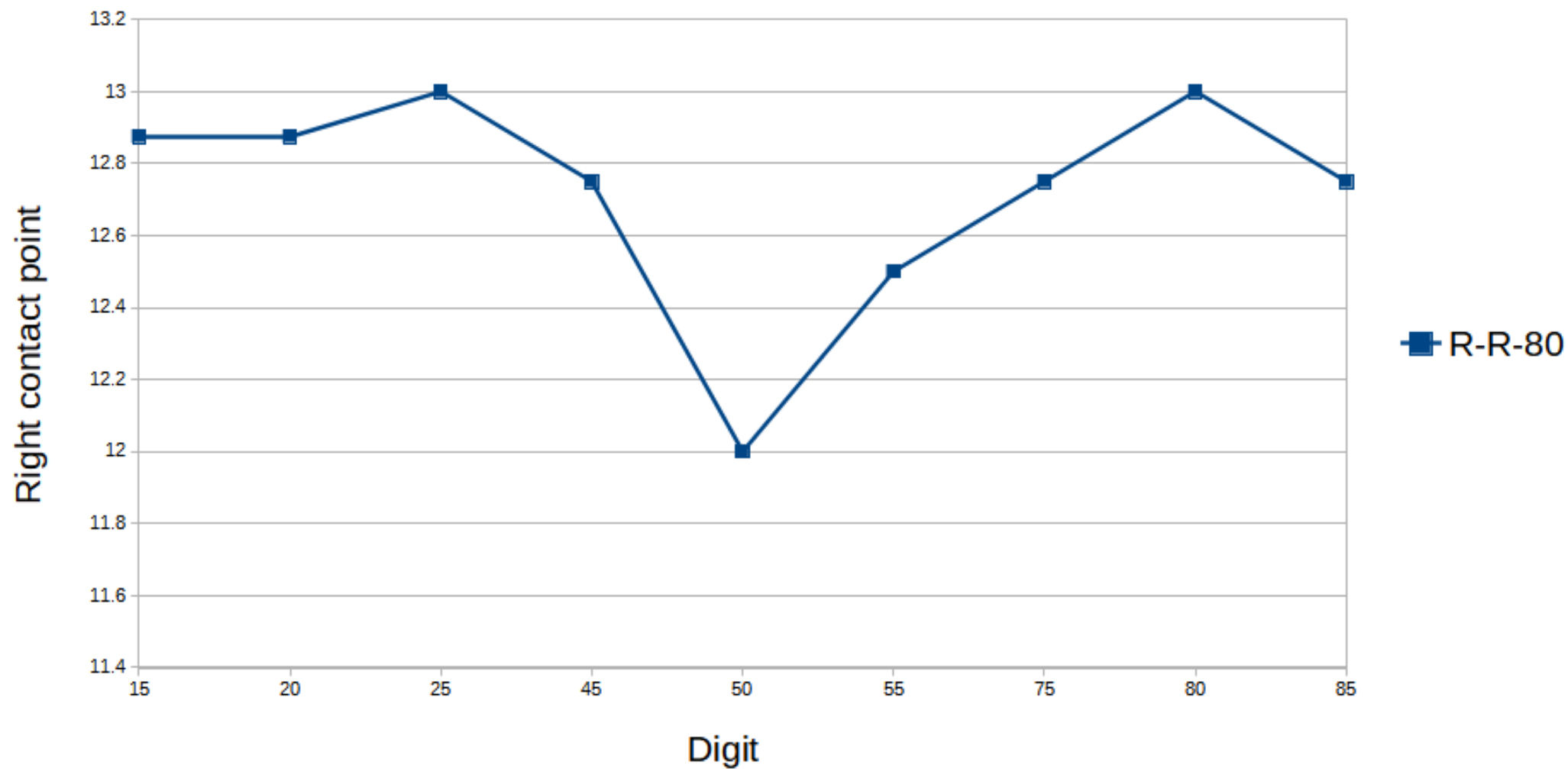
- We need to test which wheel is the lowest point is
 - We dial:
 - 80L 80L 70R 13
 - 70R 80L 80L 12.5
 - 80L 70R 80L 12.5

Manipulation process

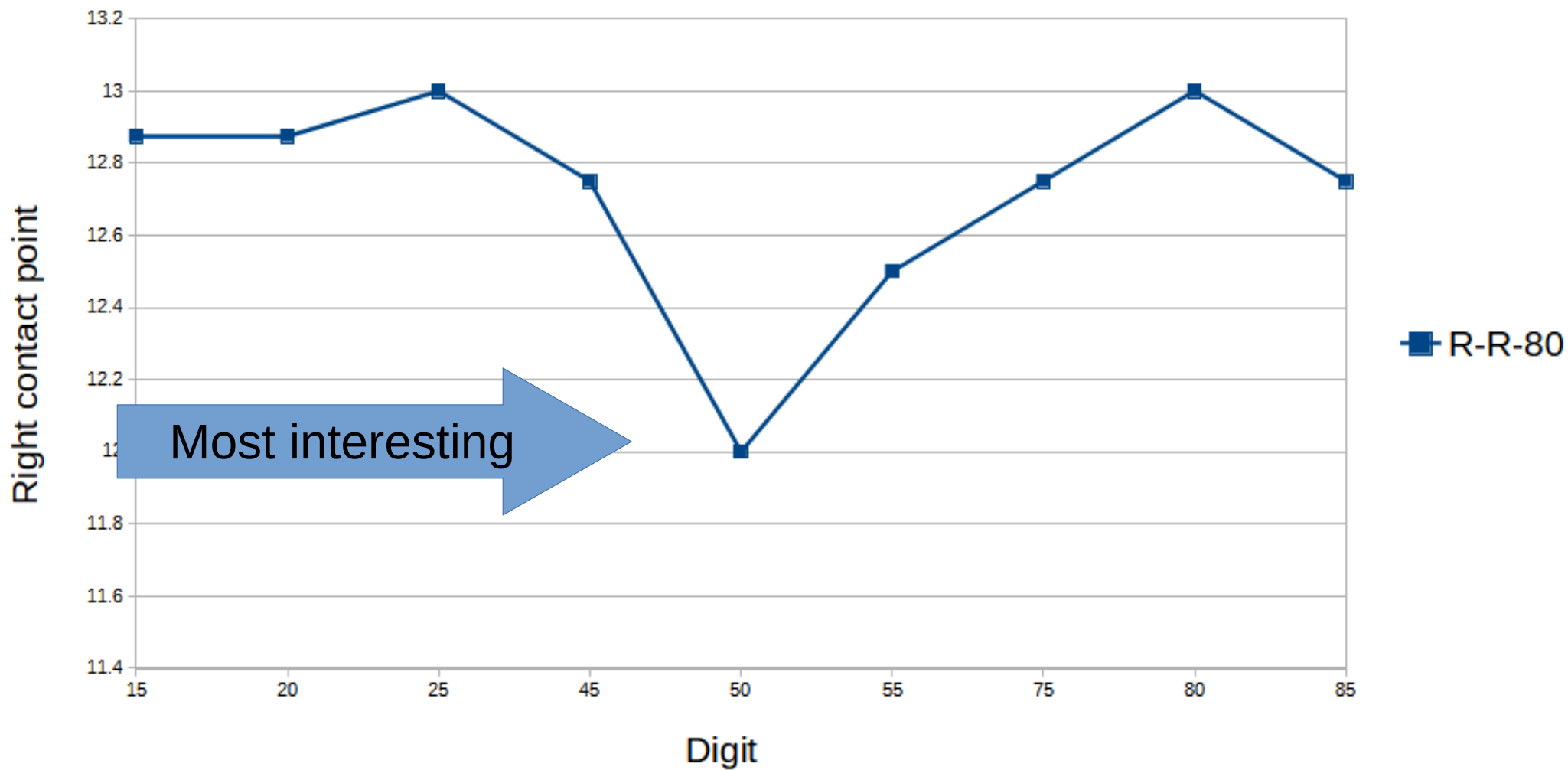
- With 80 left on the third wheel we make a new graph: Right Right 80L



Second graph: S&G 6730



Second graph: S&G 6730

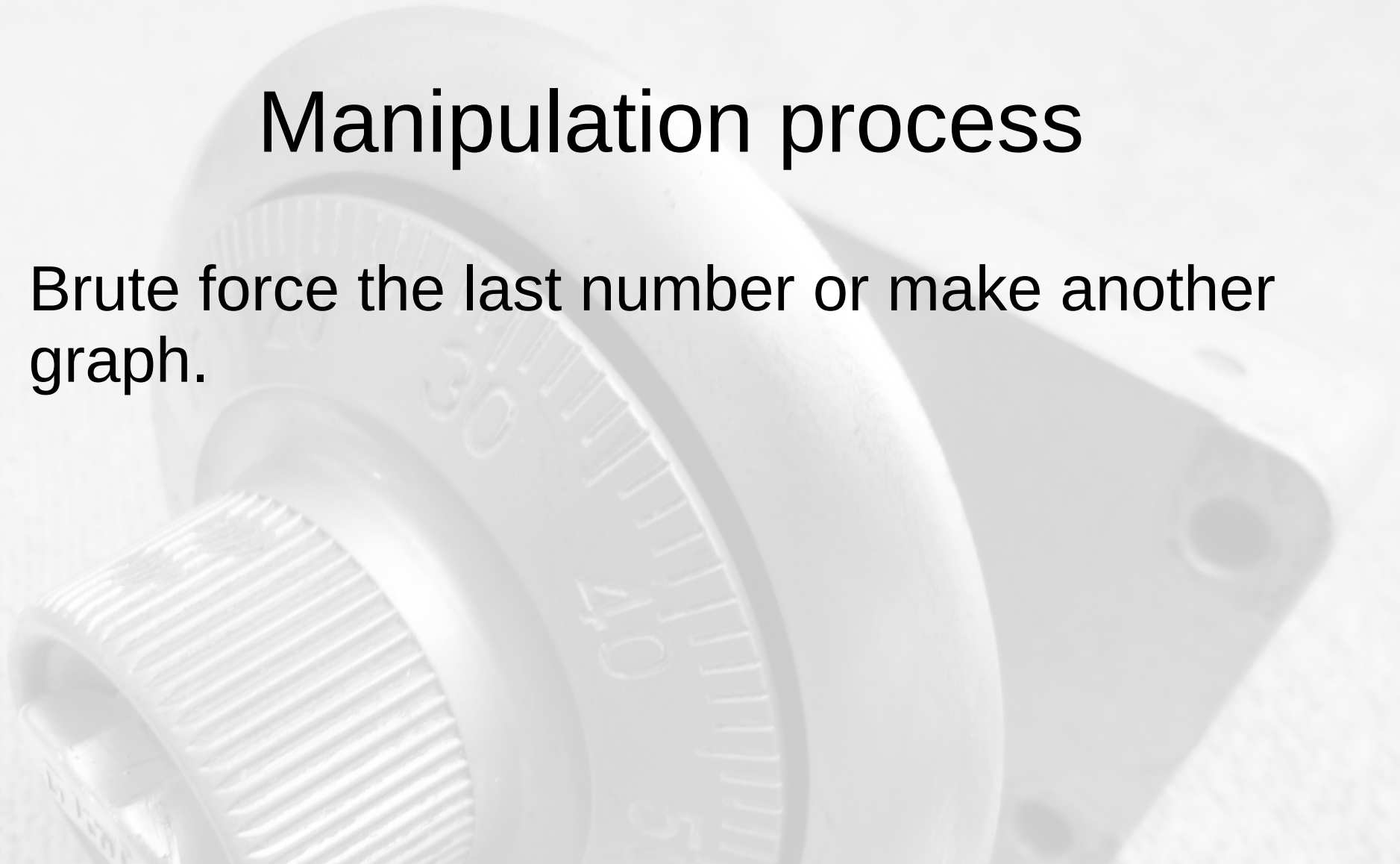


Manipulation process

- 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

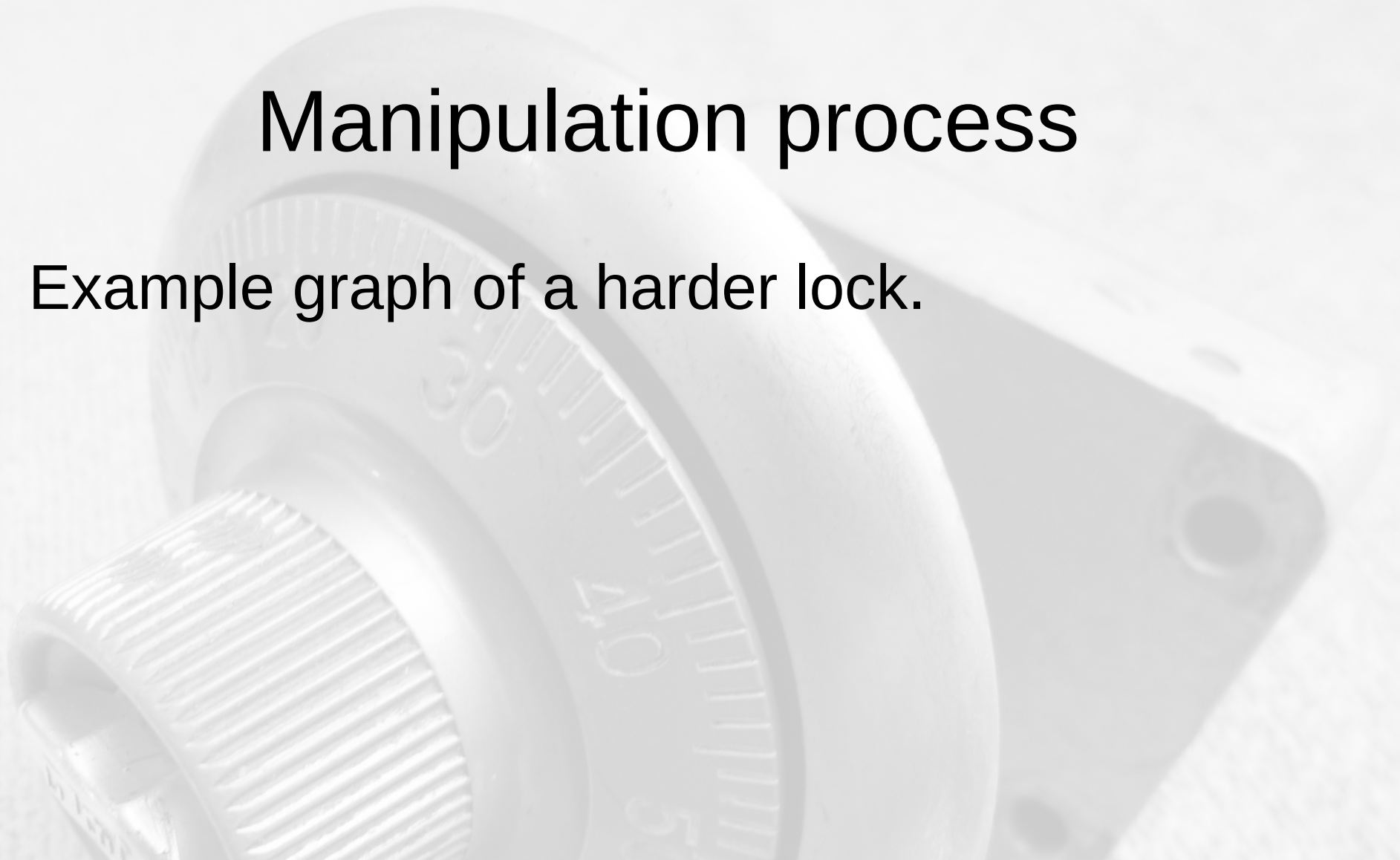
- Brute force the last number or make another graph.
- Brute forcing **L 50R 80L** the lock opened at **20**, giving us the solution **20L 50R 80L**.

Manipulation process

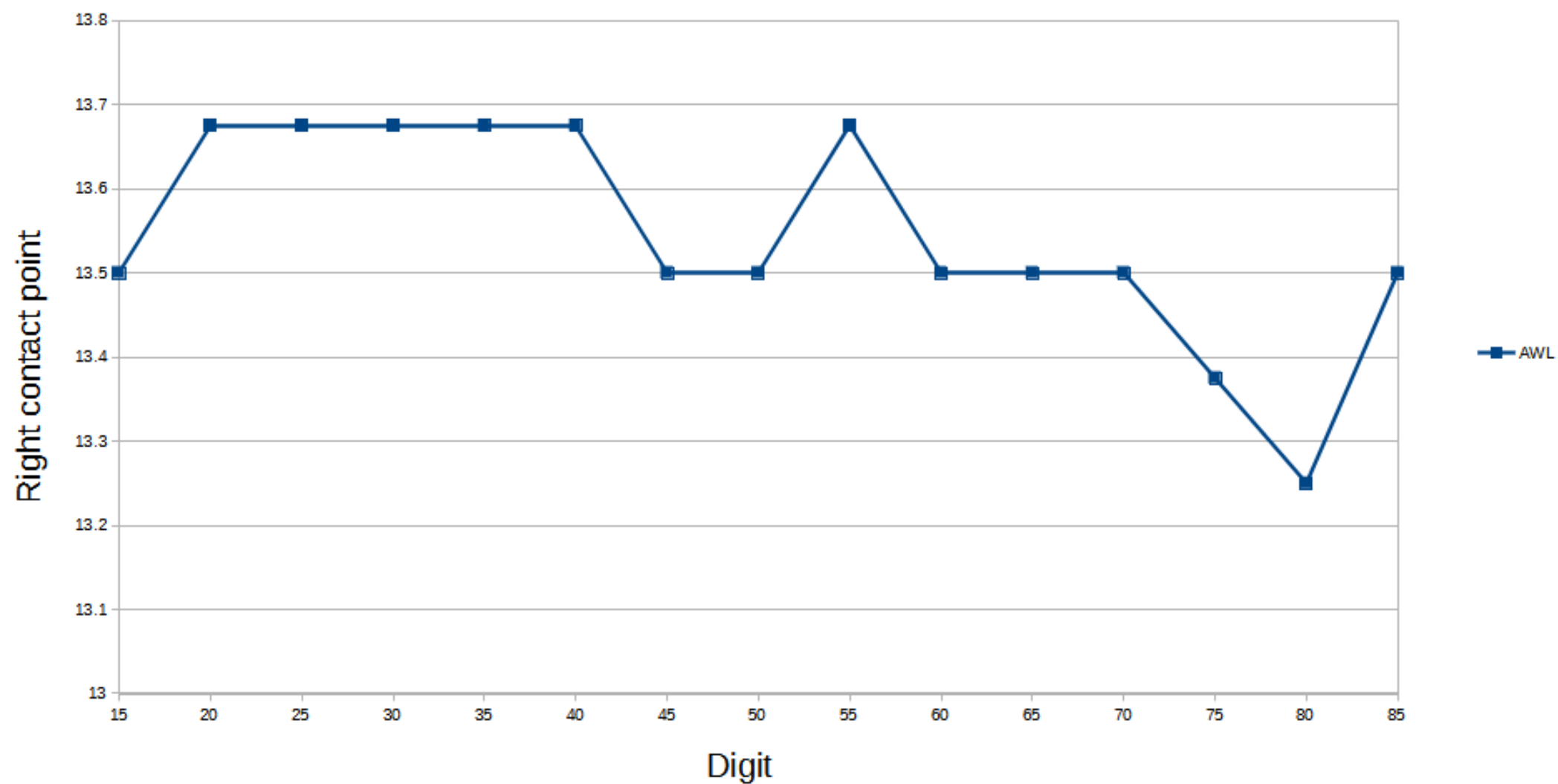
- Note the dialing direction
- Check every n numbers
- Be consistent in dialing/graphing
- Progress:
 - new low reading, this does not have to be a gate.

Manipulation process

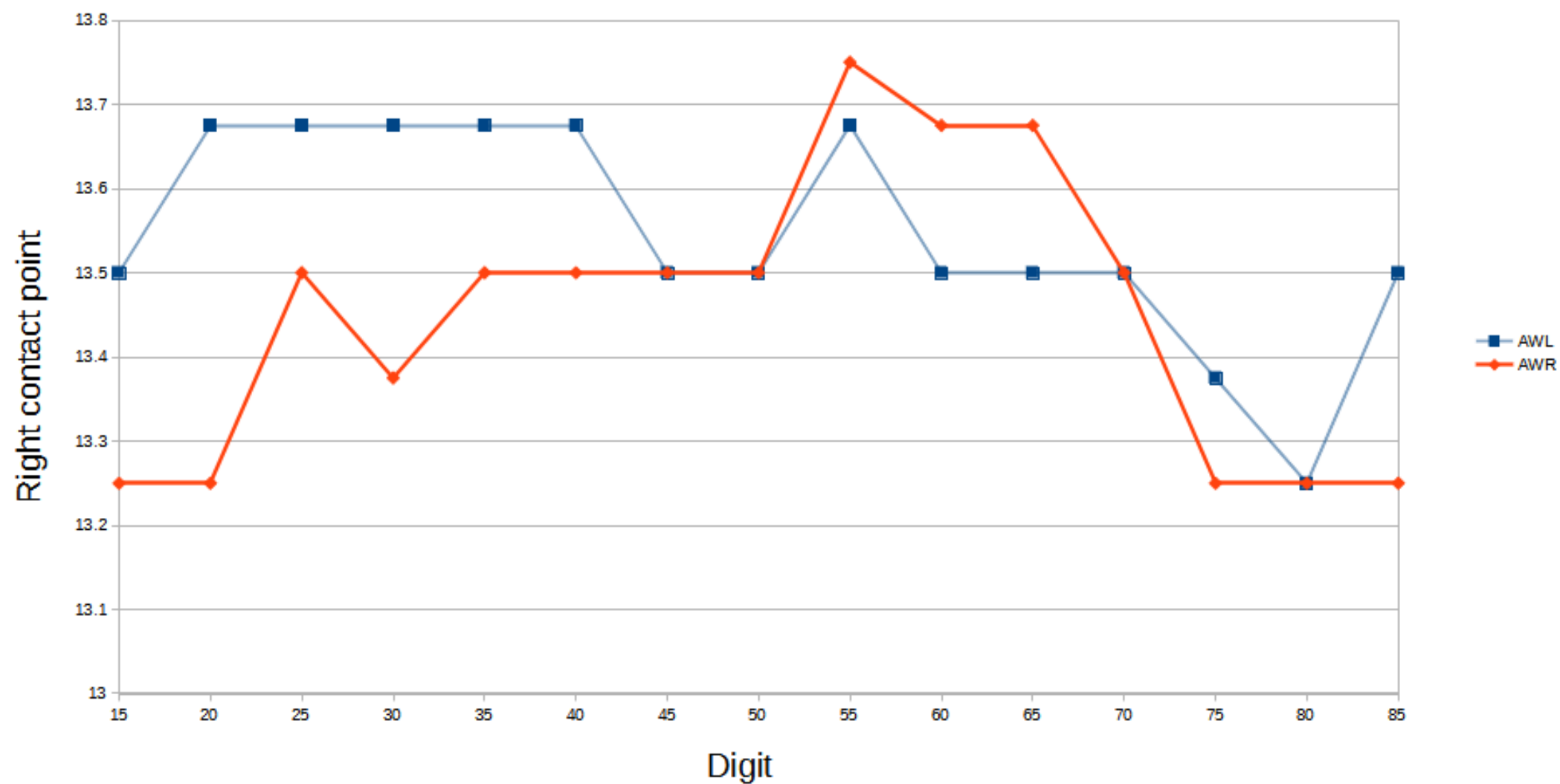
- Example graph of a harder lock.



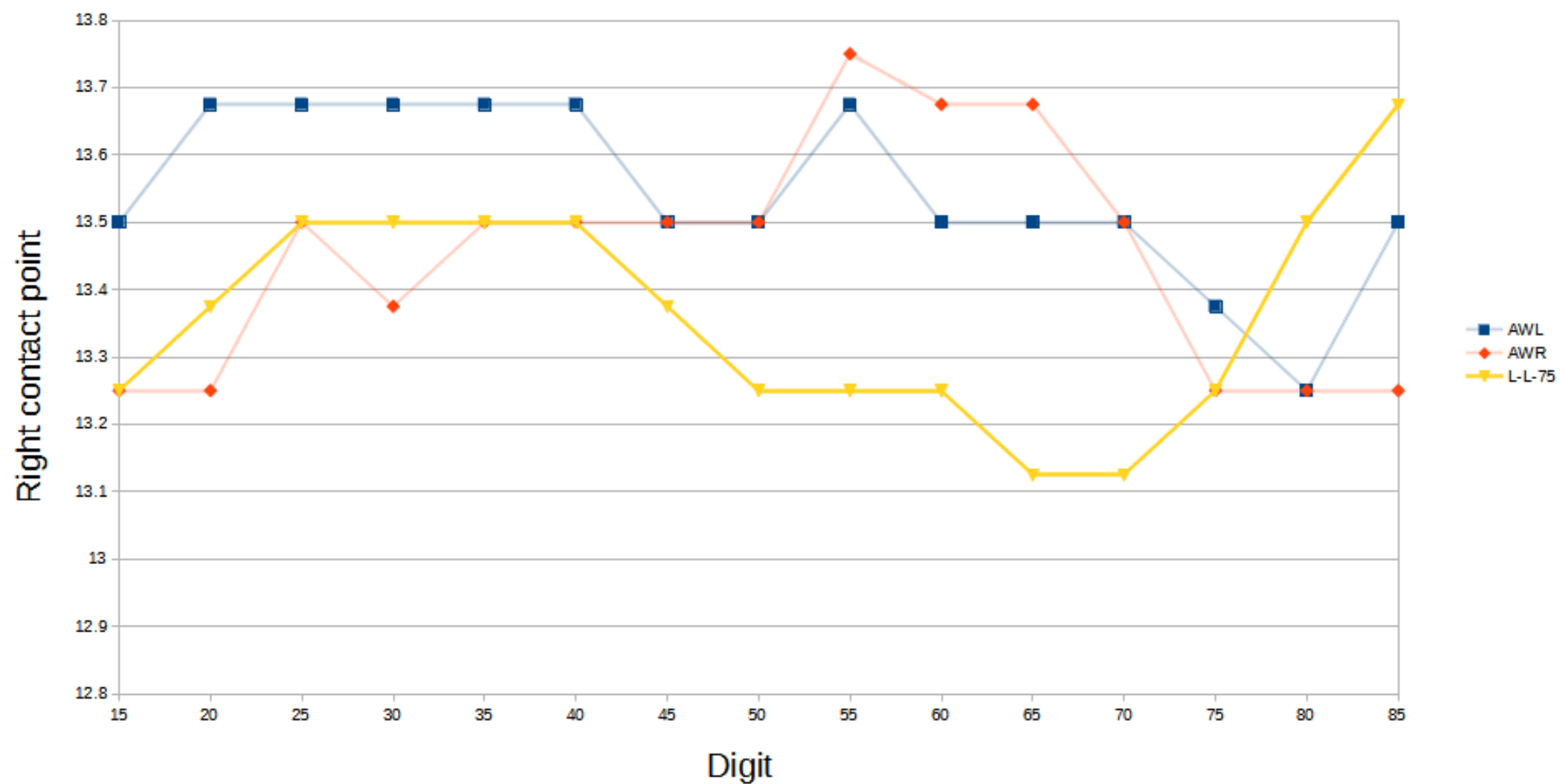
Graph 1: Difficult lock



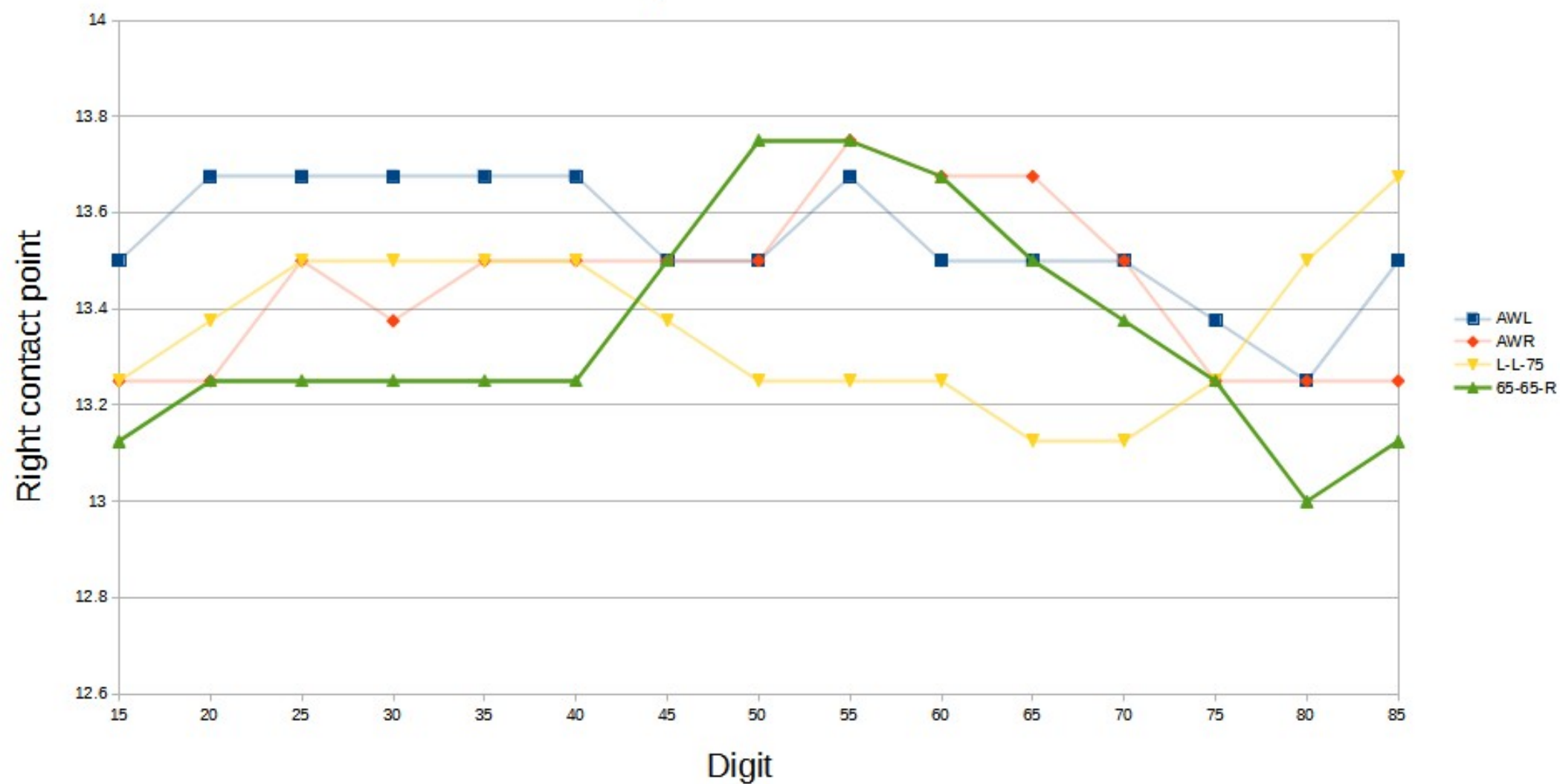
Graph 2: Difficult lock



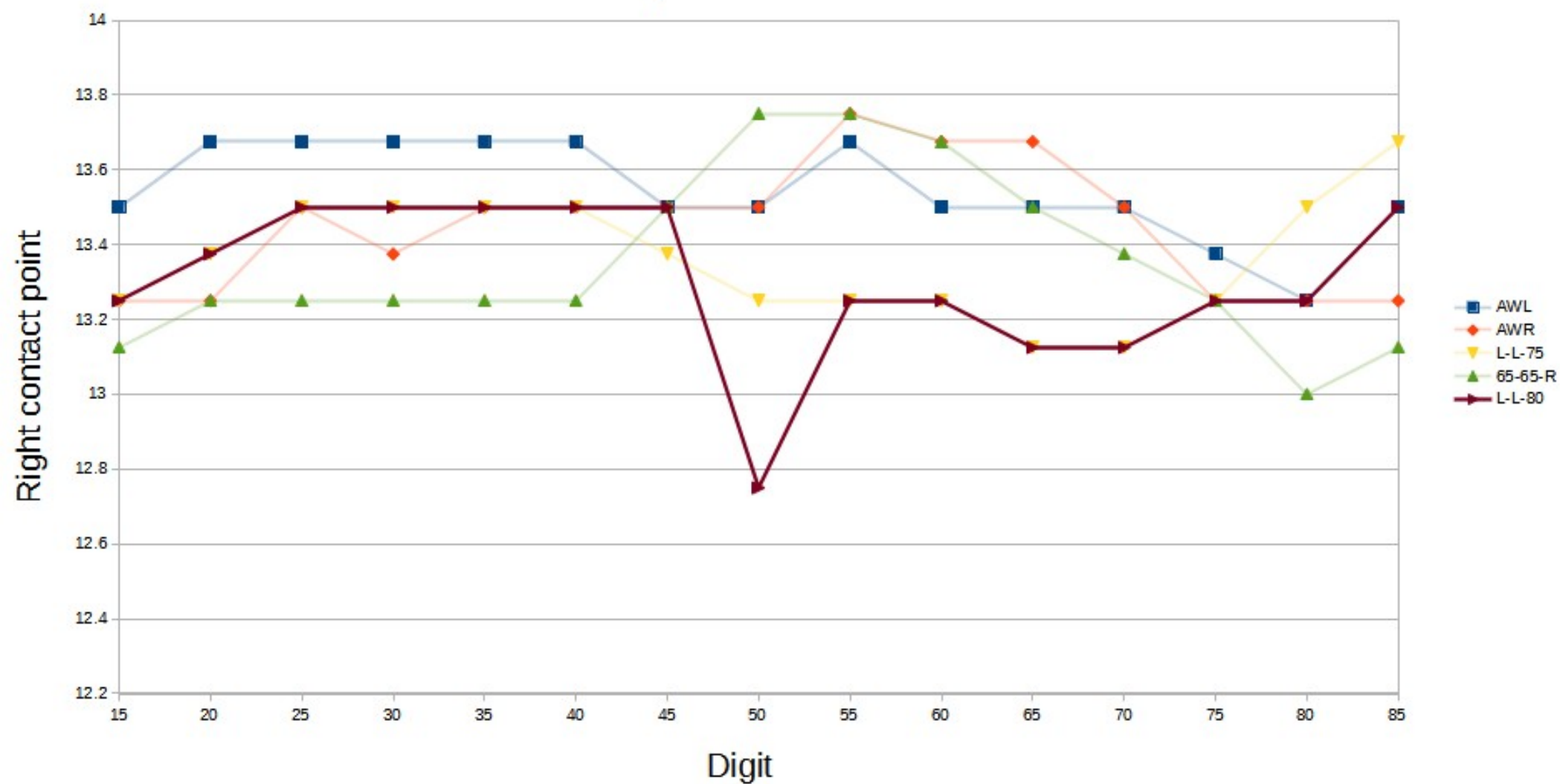
Graph 3: Difficult lock



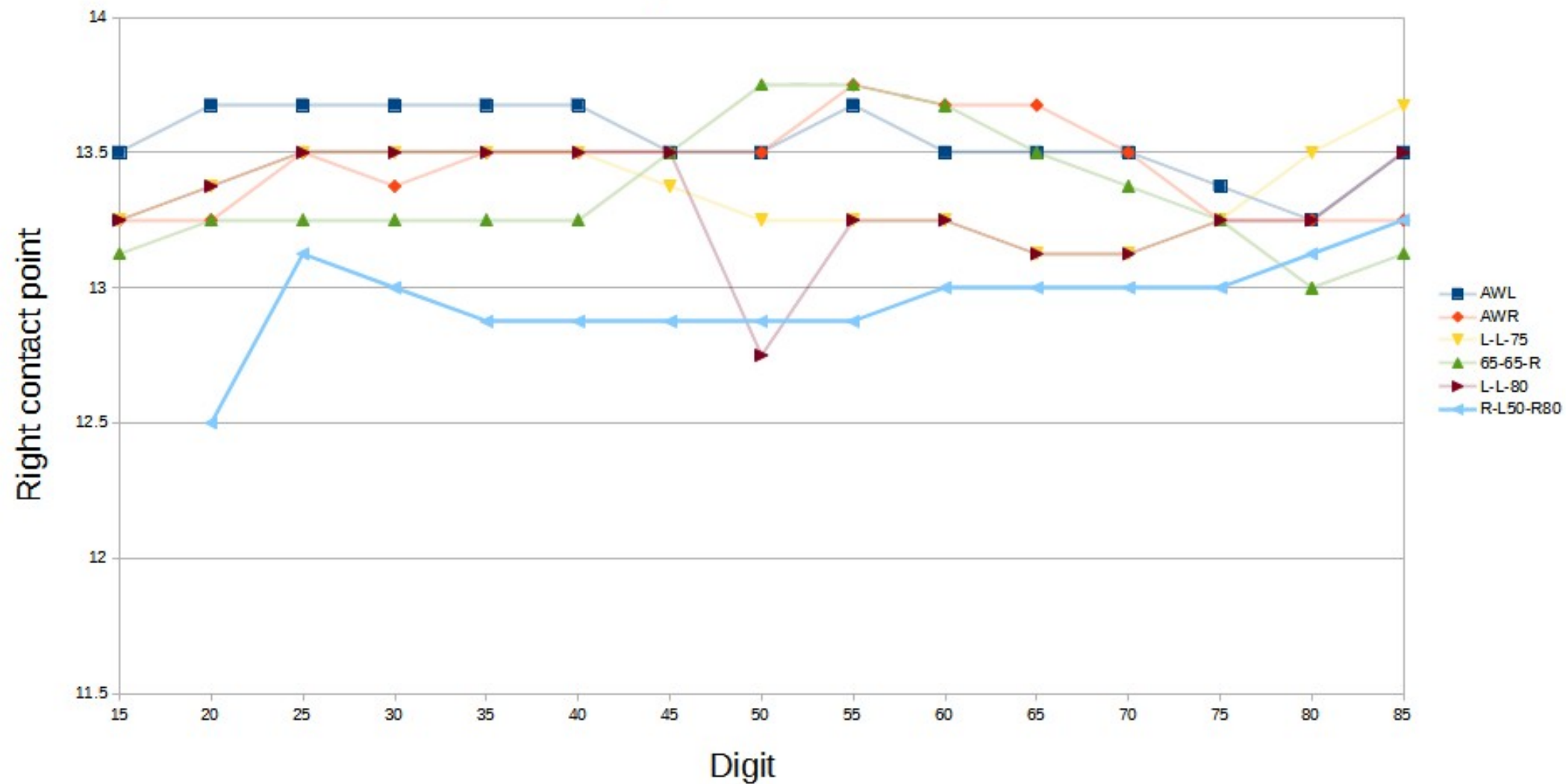
Graph 4: Difficult lock



Graph 5: Difficult lock

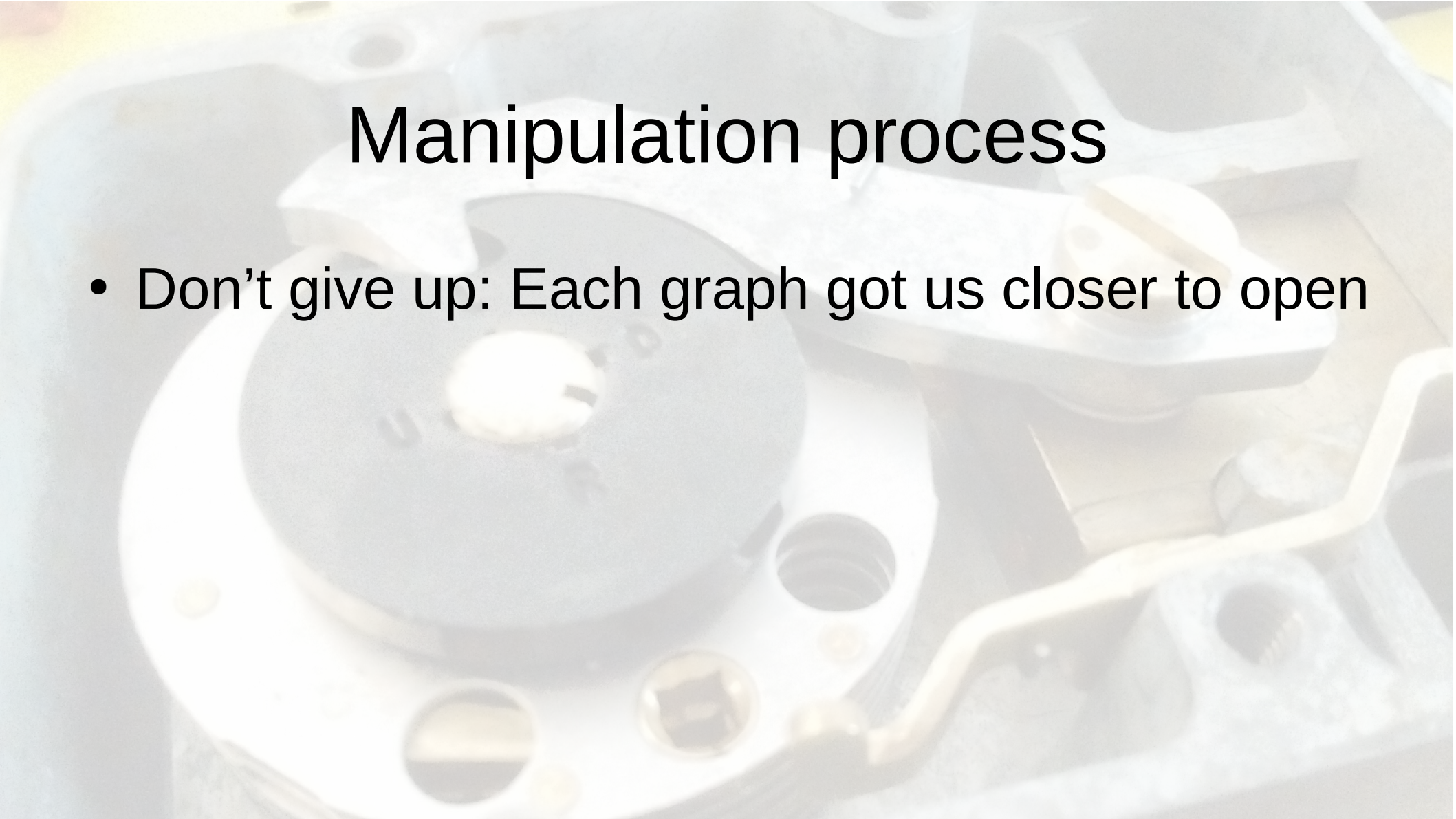


Graph 6: Difficult lock



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

L81, R96, L28

S&S
Safe & Sound Co.

Virtual lock to practice

Play

Change Lock

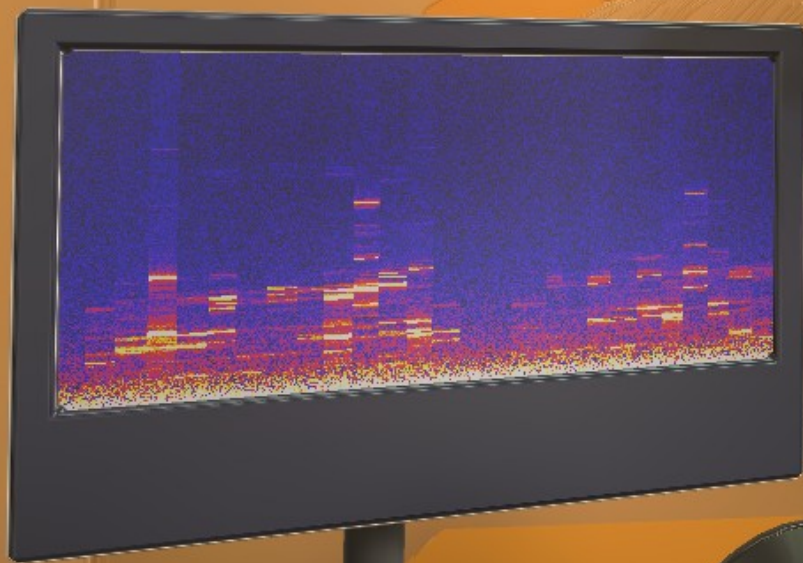
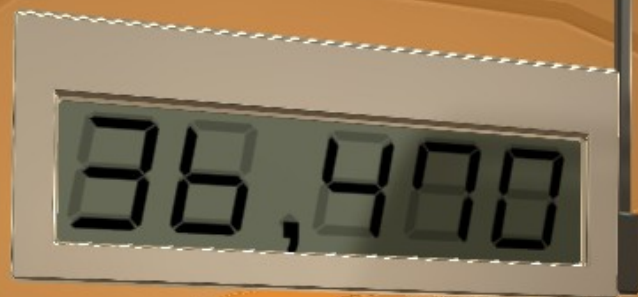
Tutorial

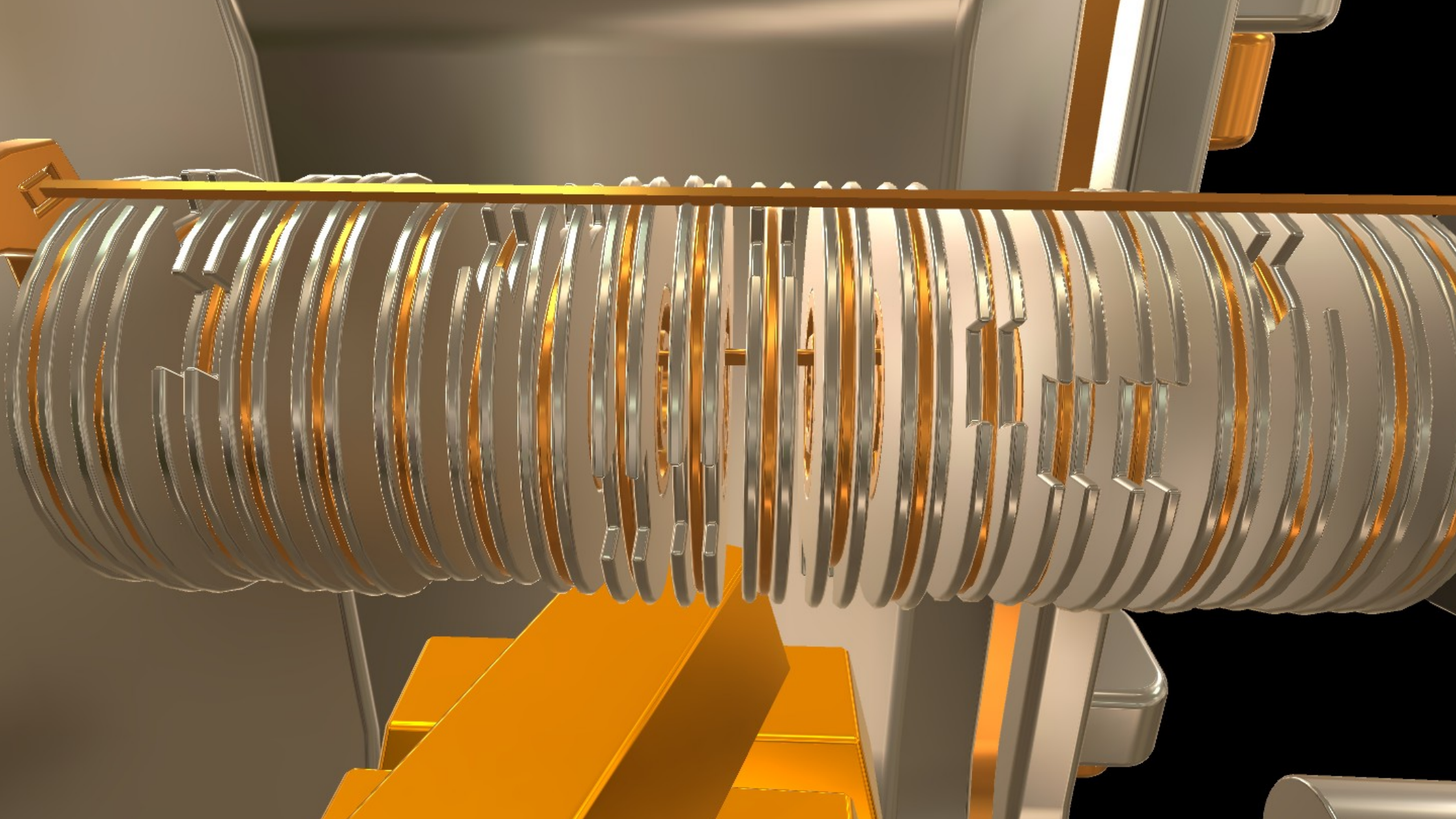
Settings

Credits

Quit Game



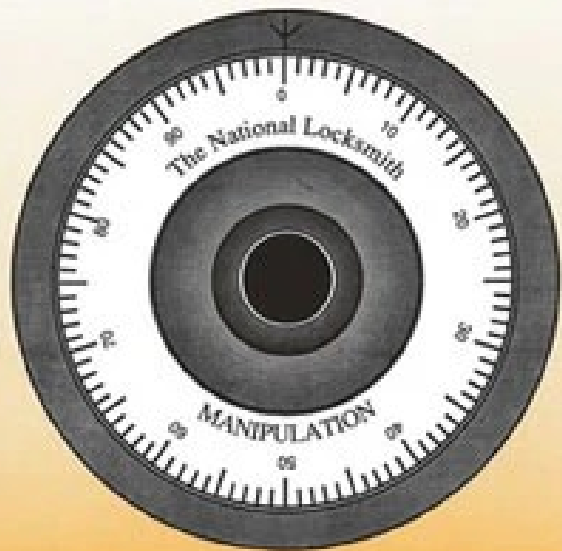




The National Locksmith

Guide to:

M·A·N·I·P·U·L·A·T·I·O·N

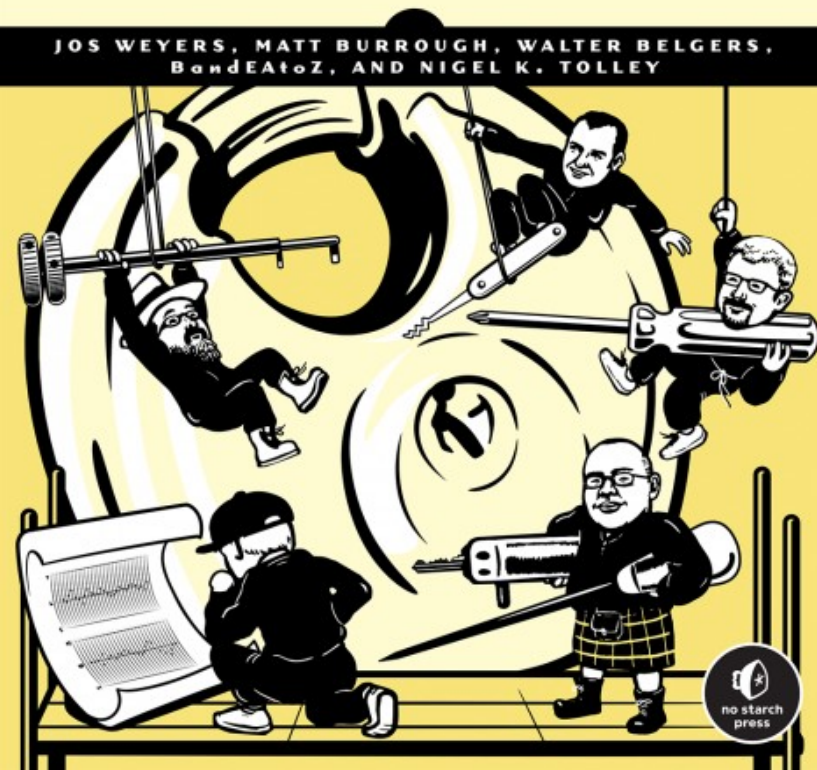


by Robert Gene Sieveking

LOCKSPORT

A HACKER'S GUIDE TO LOCK PICKING,
IMPRESSIONING, AND SAFE CRACKING

JOS WEYERS, MATT BURROUGH, WALTER BELGERS,
BandeAtoZ, AND NIGEL K. TOLLEY



The end

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

Jan-willem@Toool.nl

@jworm22