Experiment driven lockpicking



Jan-Willem Markus
Hacker Hotel 2023



Follow

Jan-Willem CCX

@jwrm22

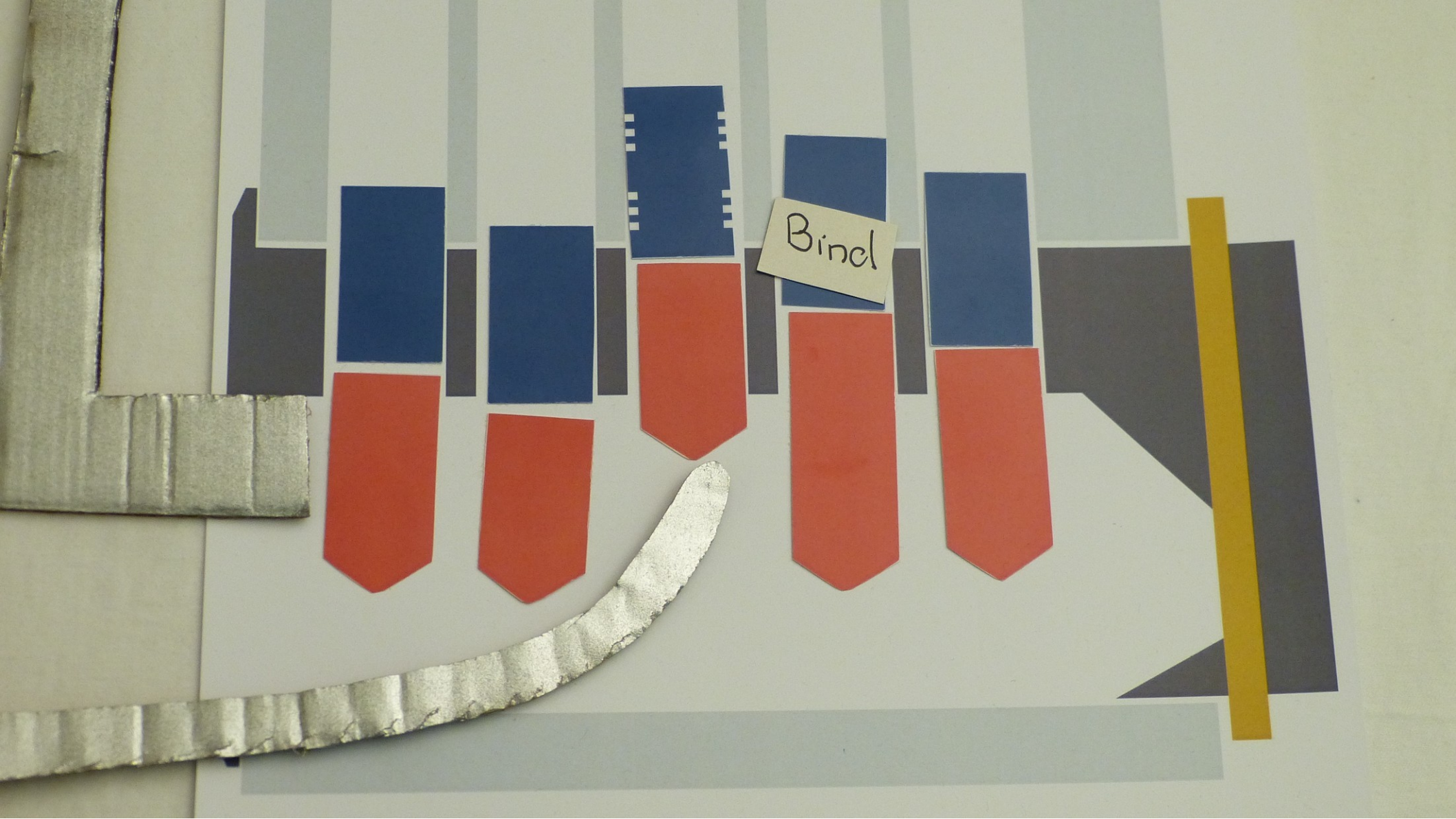
Nerd, Board member of TOOOL, Electrical engineer, Hardware Hacker #Cyber



The Open Organisation Of Lockpickers

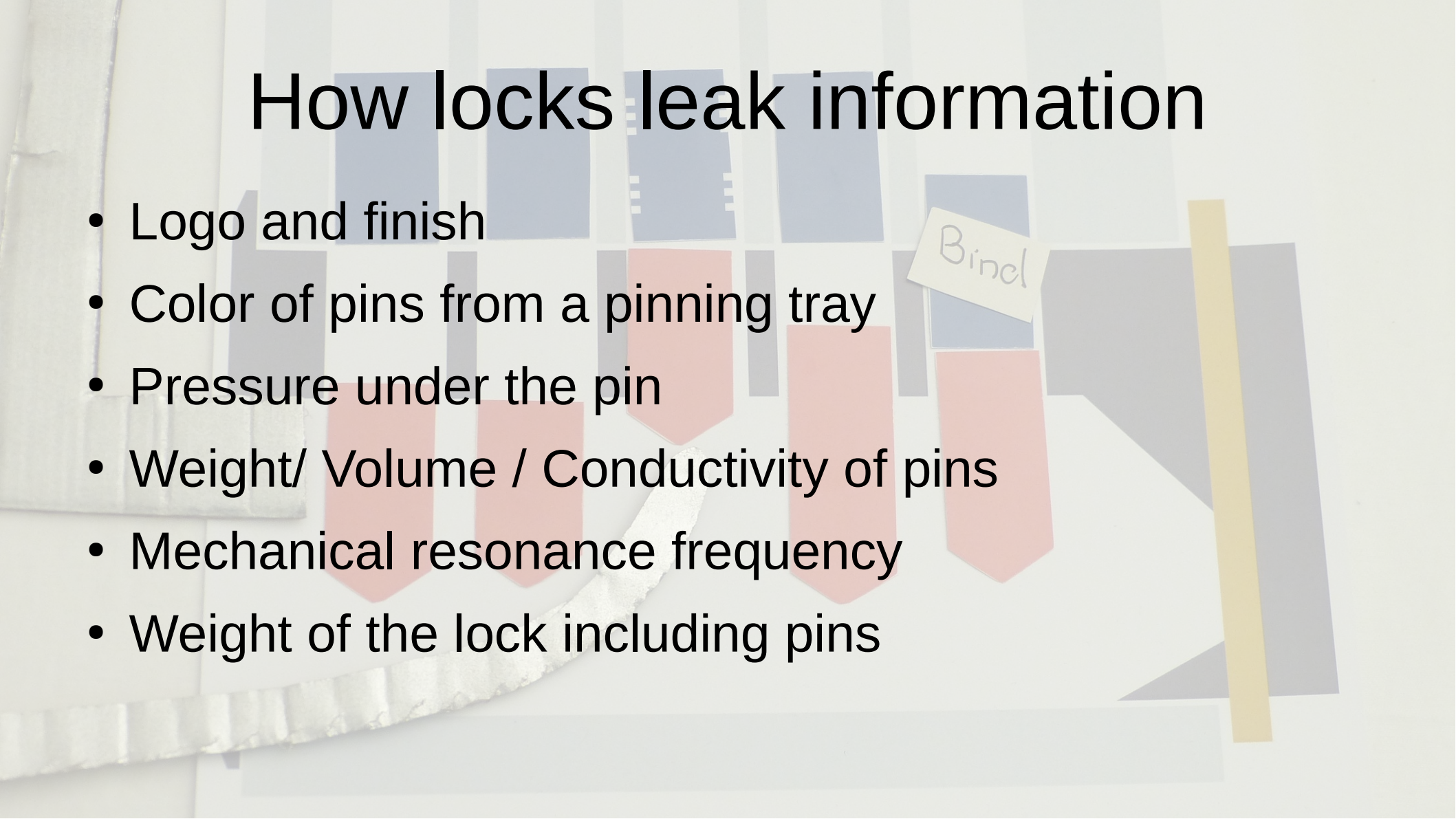
Side channels

- Unintentional information leakage
  - Binding order
  - Impressioning marks
  - Core rotation
  - Sound
  - Etc...


Bind

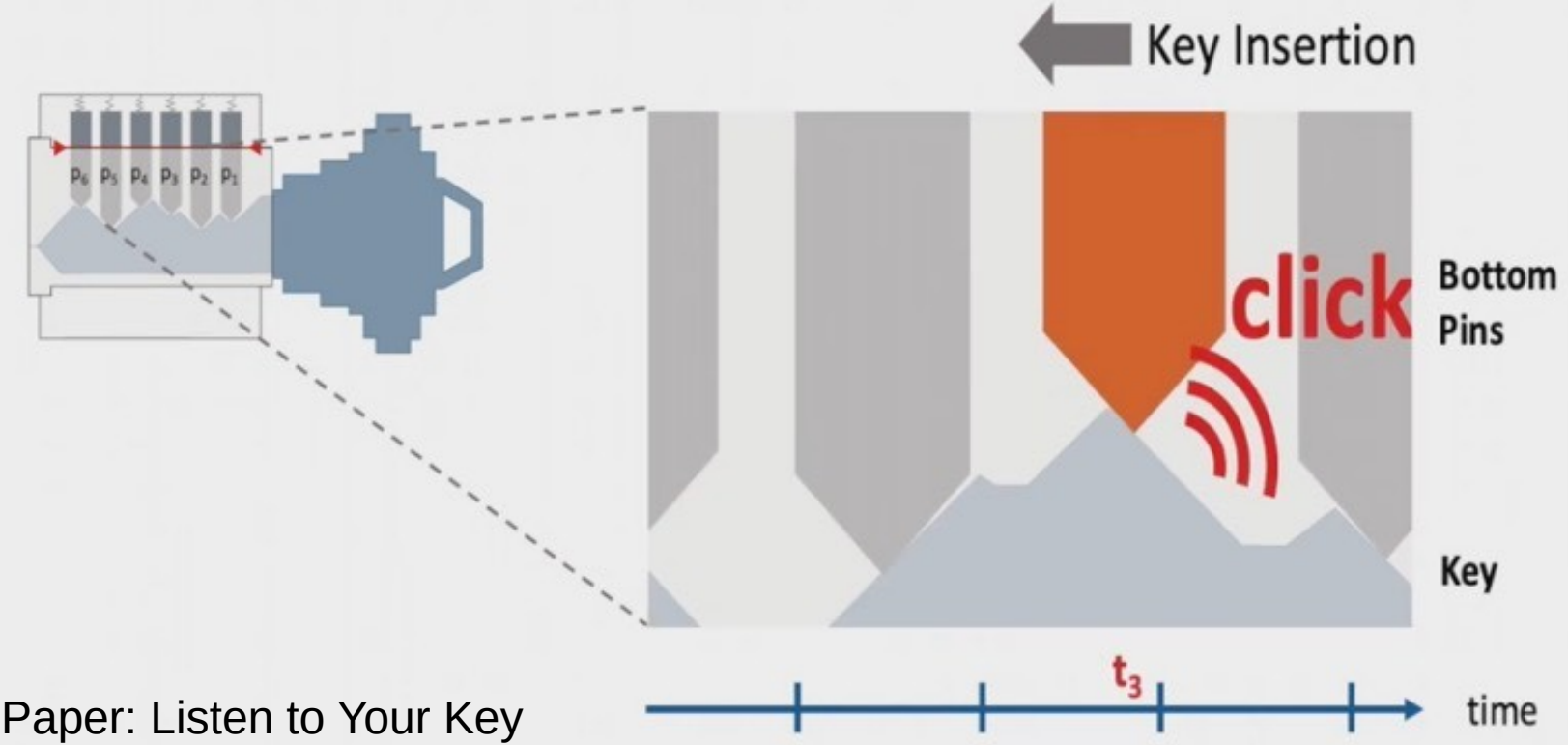
How locks leak information

- Logo and finish
- Color of pins from a pinning tray
- Pressure under the pin
- Weight/ Volume / Conductivity of pins
- Mechanical resonance frequency
- Weight of the lock including pins



Understanding the Cause of Sound

- When the pin falls off a key-ridge, “click” sound occurs



Paper: Listen to Your Key

https://dl.acm.org/doi/abs/10.1145/3376897.3377853

Sicherheits-Schließzylinder
Security locking cylinder
Cylindres et serrures de sécurité

Schließanlagen
Master Key Systems
Installations de fermeture

DOM

Garage

we domore for security

dom-group.eu

we domore for security

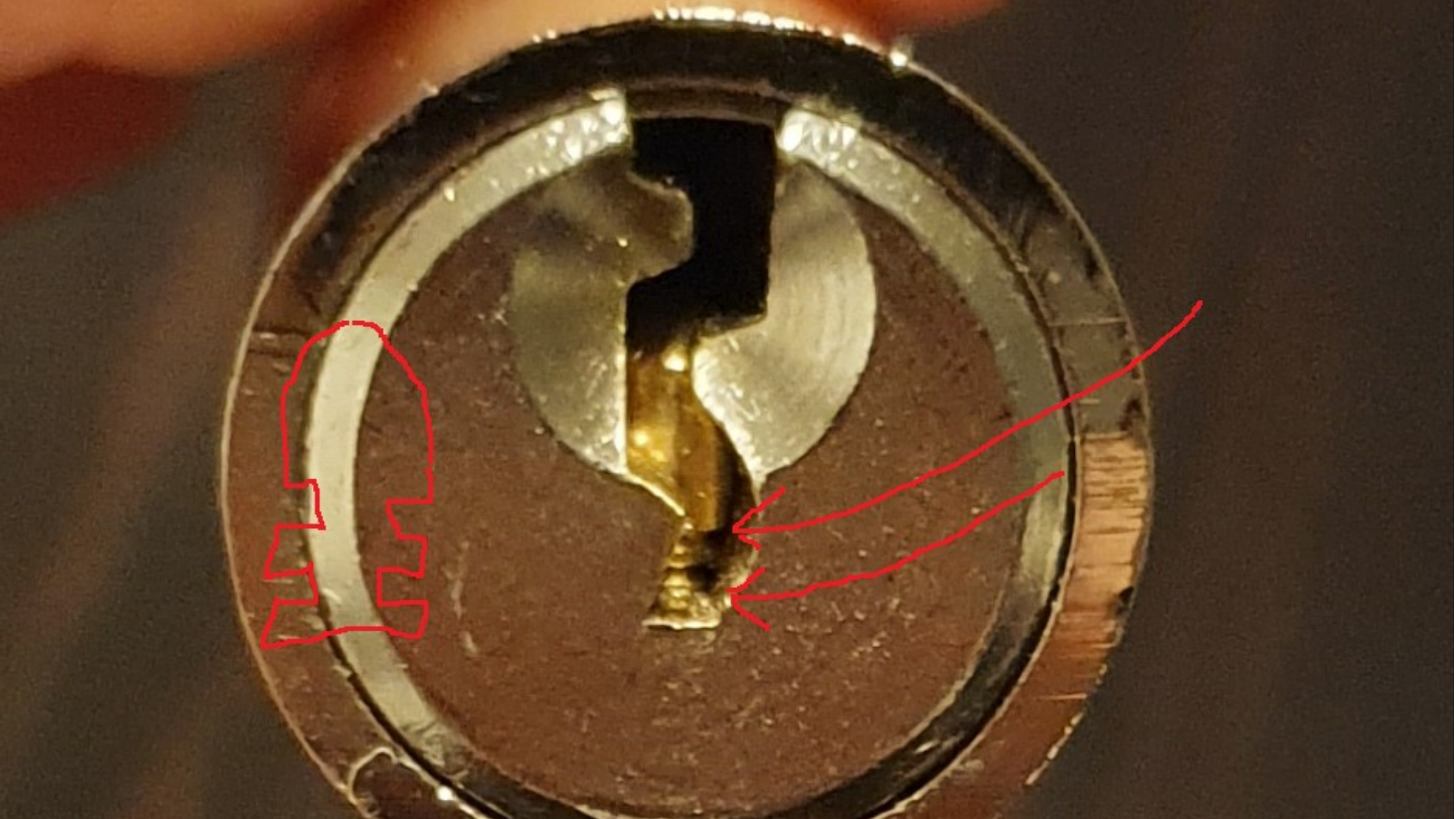
dom-group.eu

Sicherheits-Schließzylinder
Security locking cylinder
Cylindres et serrures de sécurité

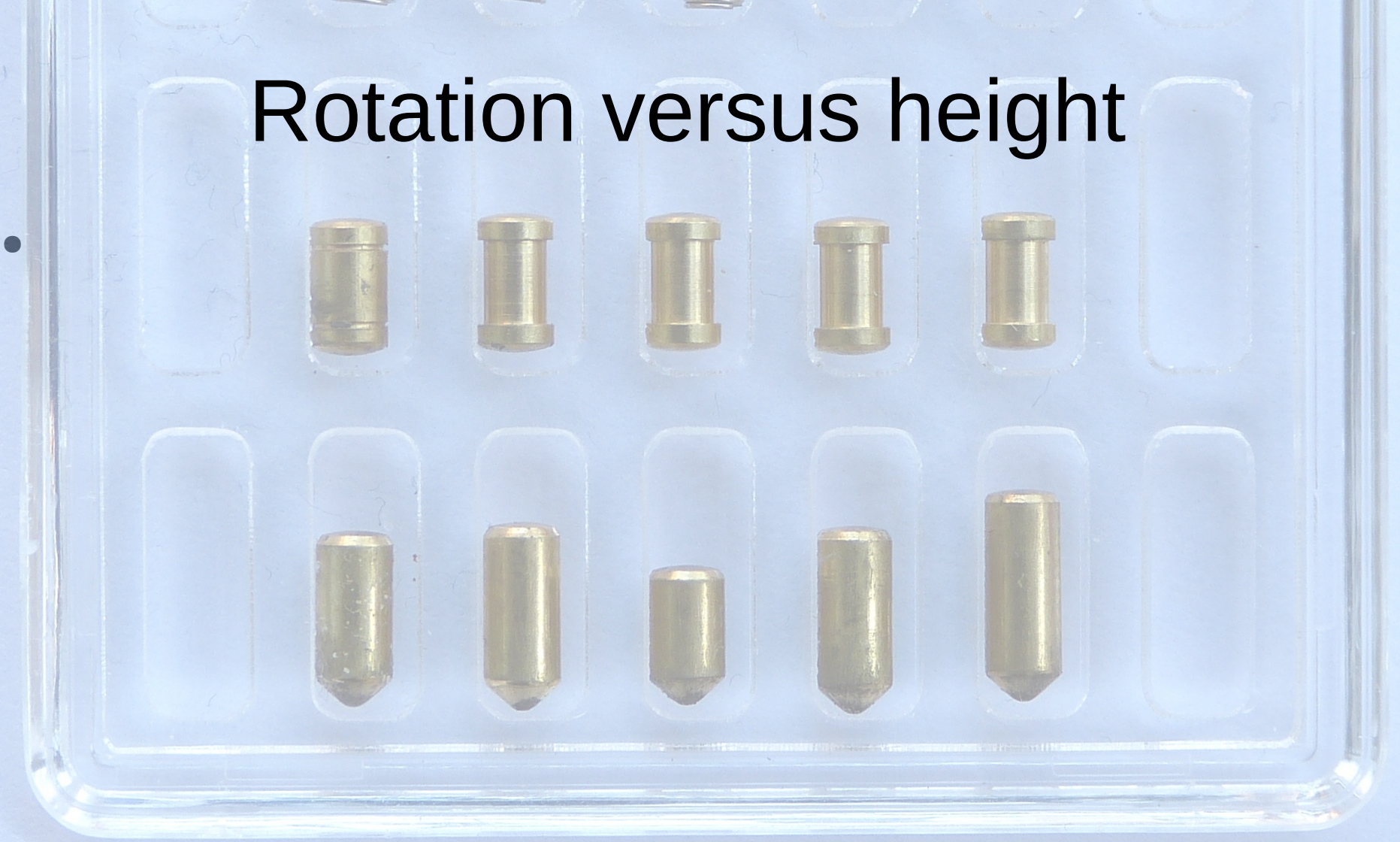
Schließanlagen
Master Key Systems
Installations de fermeture

DOM

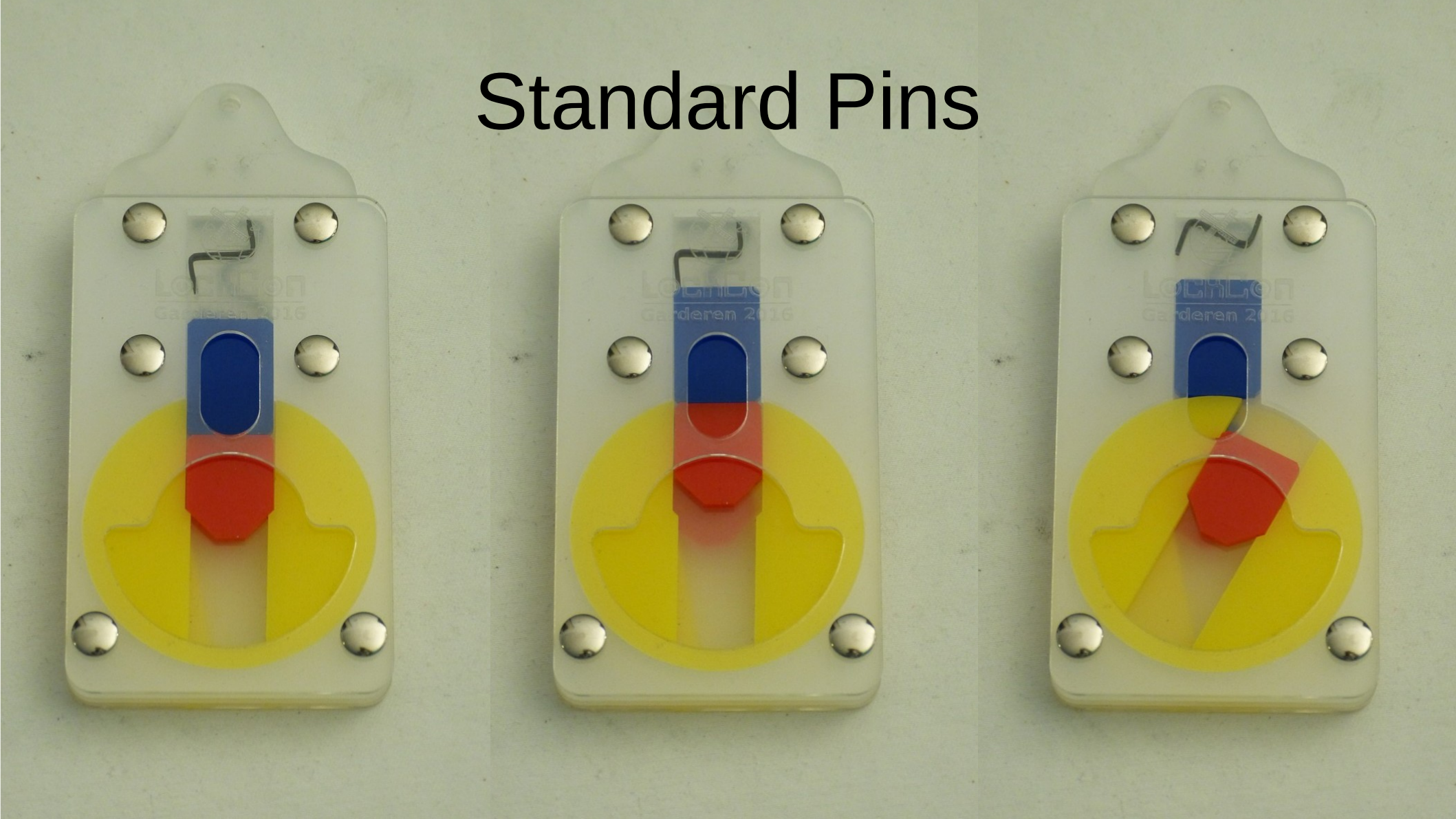

HK14276
DOM
Plura
HK14276



Rotation versus height



Standard Pins



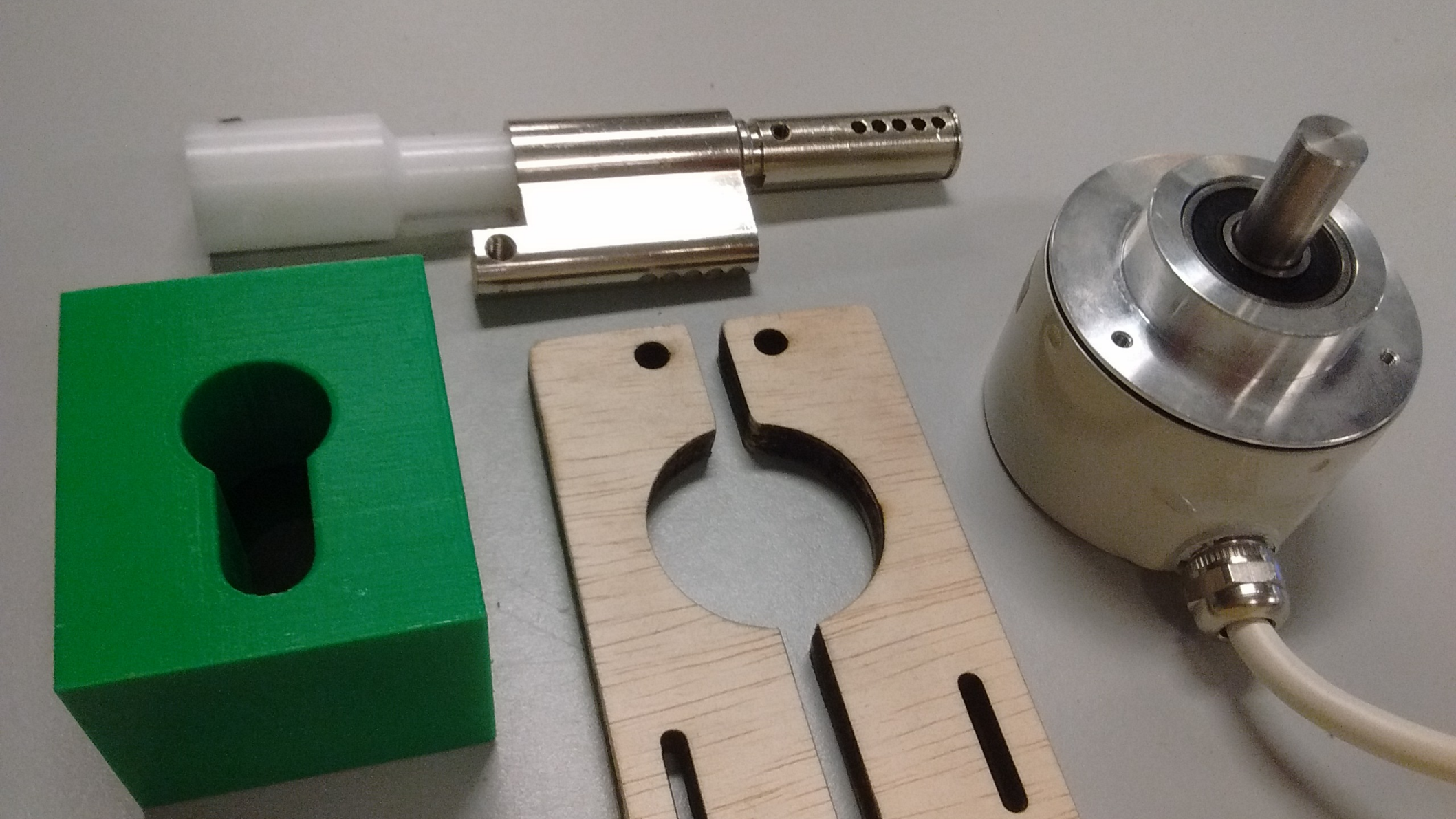
Standard Pins



Sputnik

Pin rotation side channel

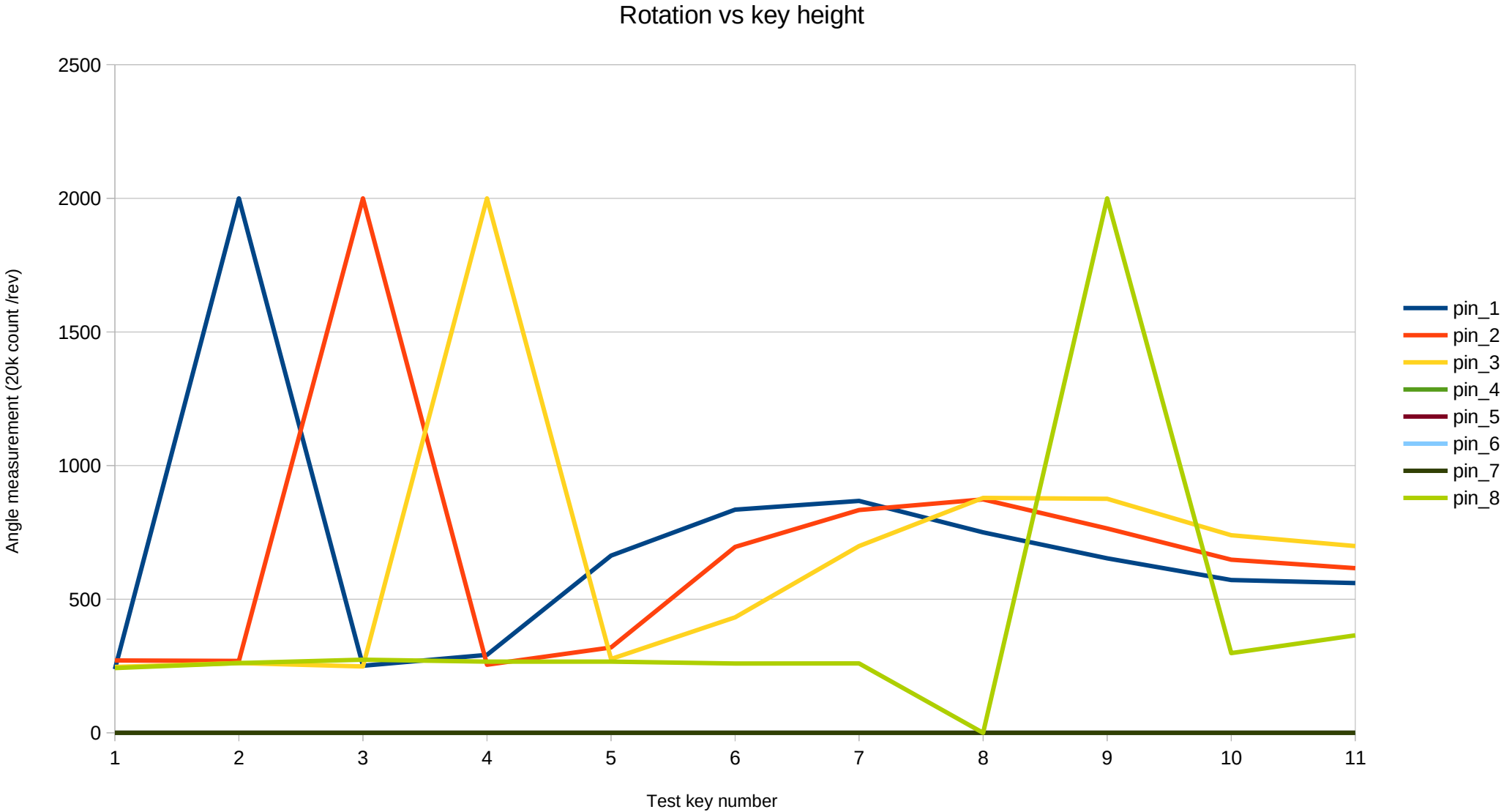
- Idea:
  - Test keys set the pins to a known position
  - Lock rotates
  - Angle is measurement
  - Calculate key options
  - Repeat until open (or try all options)

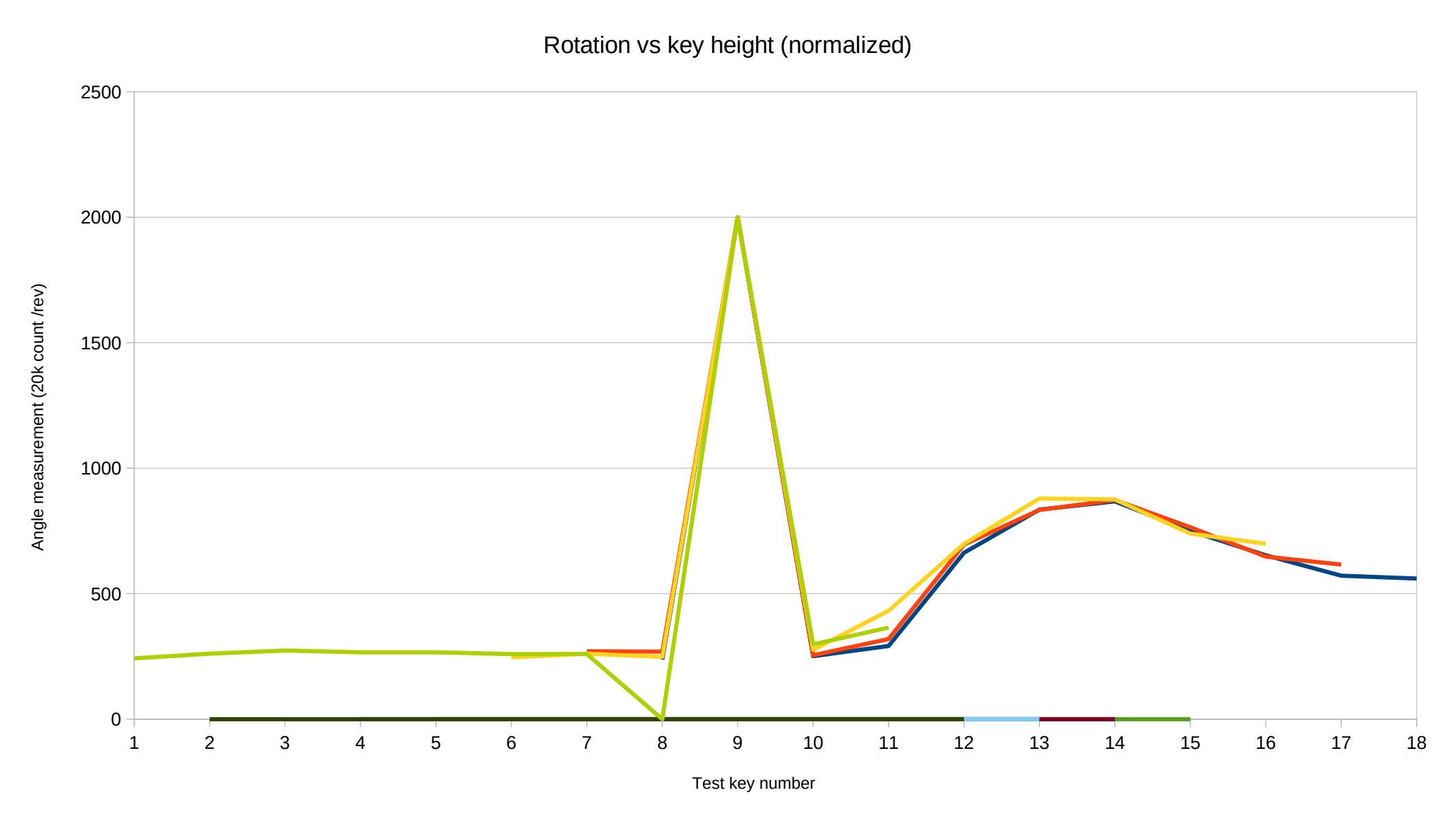


Experiments

- For every key-pin height
  - For set of test keys
    - Measure rotation angle
- Repeat for:
  - Different key pins,
  - Different drivers pins,
  - Different locks

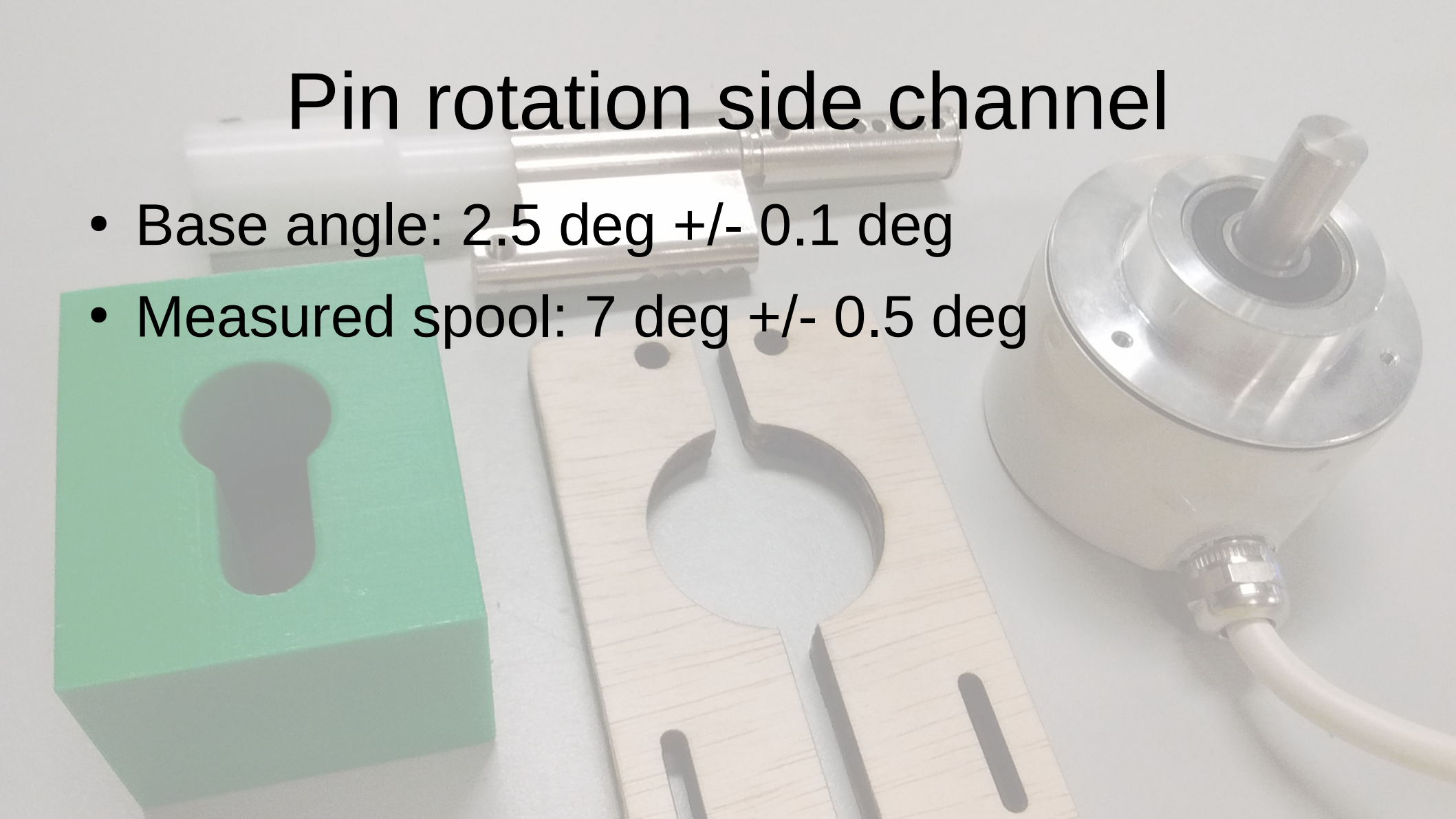



Rotation vs key height
2500
2000
1500
1000
500
0
Angle measurement (20k count /rev)
1
2
3
4
5
6
7
8
9
10
11
Test key number
pin_1
pin_2
pin_3
pin_4
pin_5
pin_6
pin_7
pin_8


Rotation vs key height (normalized)
Angle measurement (20k count /rev)
2500
2000
1500
1000
500
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
Test key number

Pin rotation side channel

- Base angle: 2.5 deg +/- 0.1 deg
- Measured spool: 7 deg +/- 0.5 deg



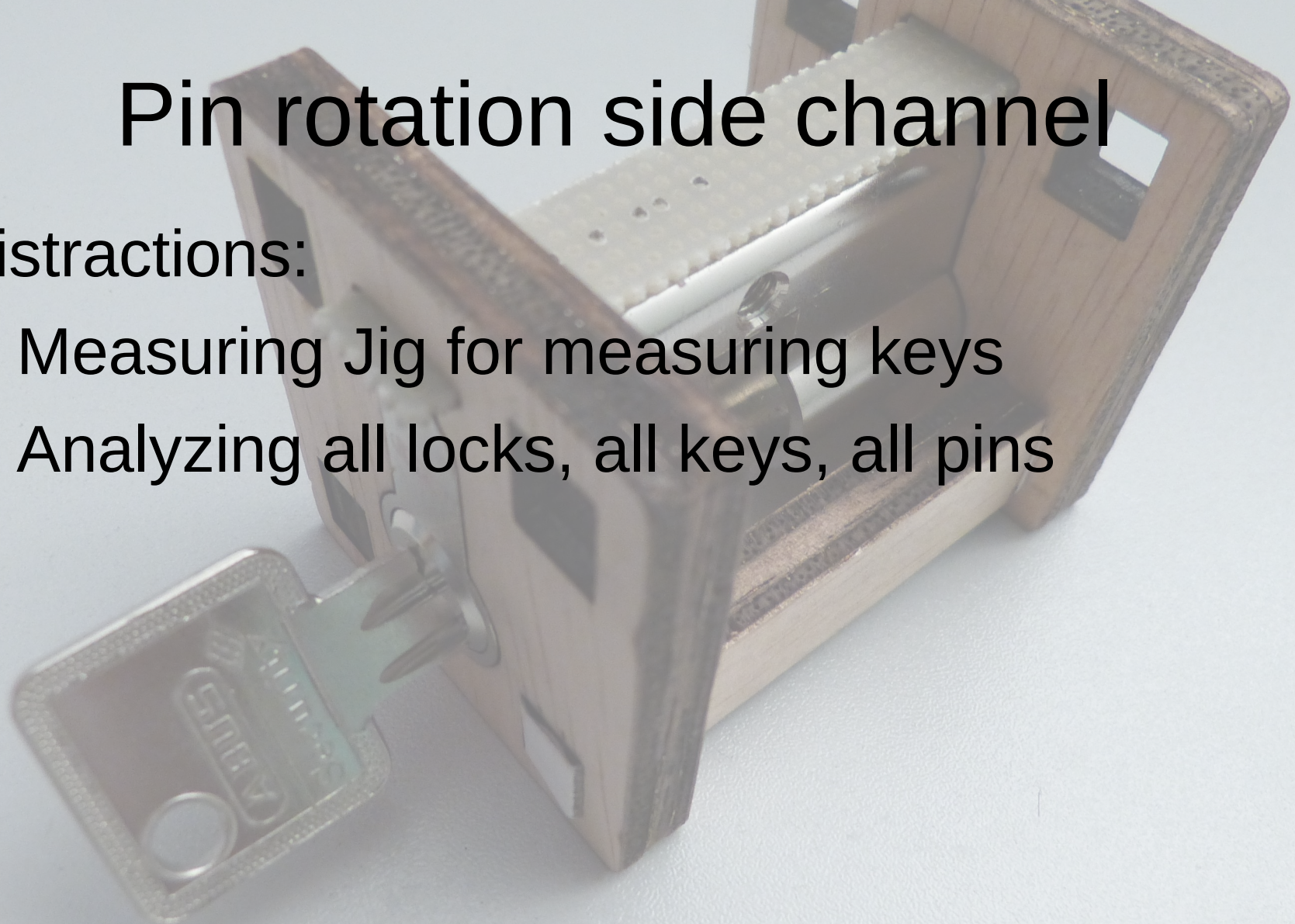
Pin rotation side channel

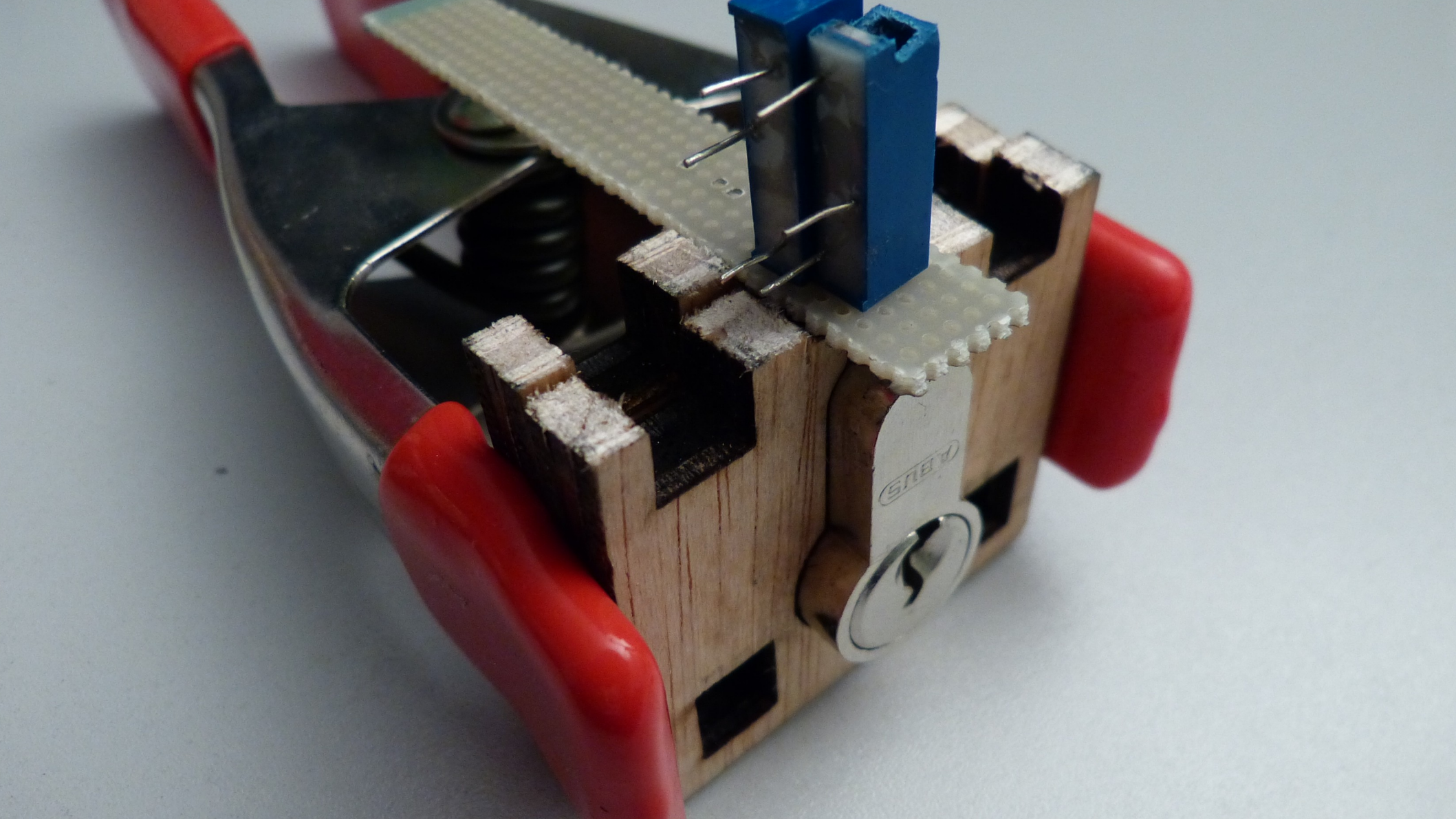
- Todo:
  - Work out the math
  - Find an efficient search algorithm
  - Build measuring tool outside the lock

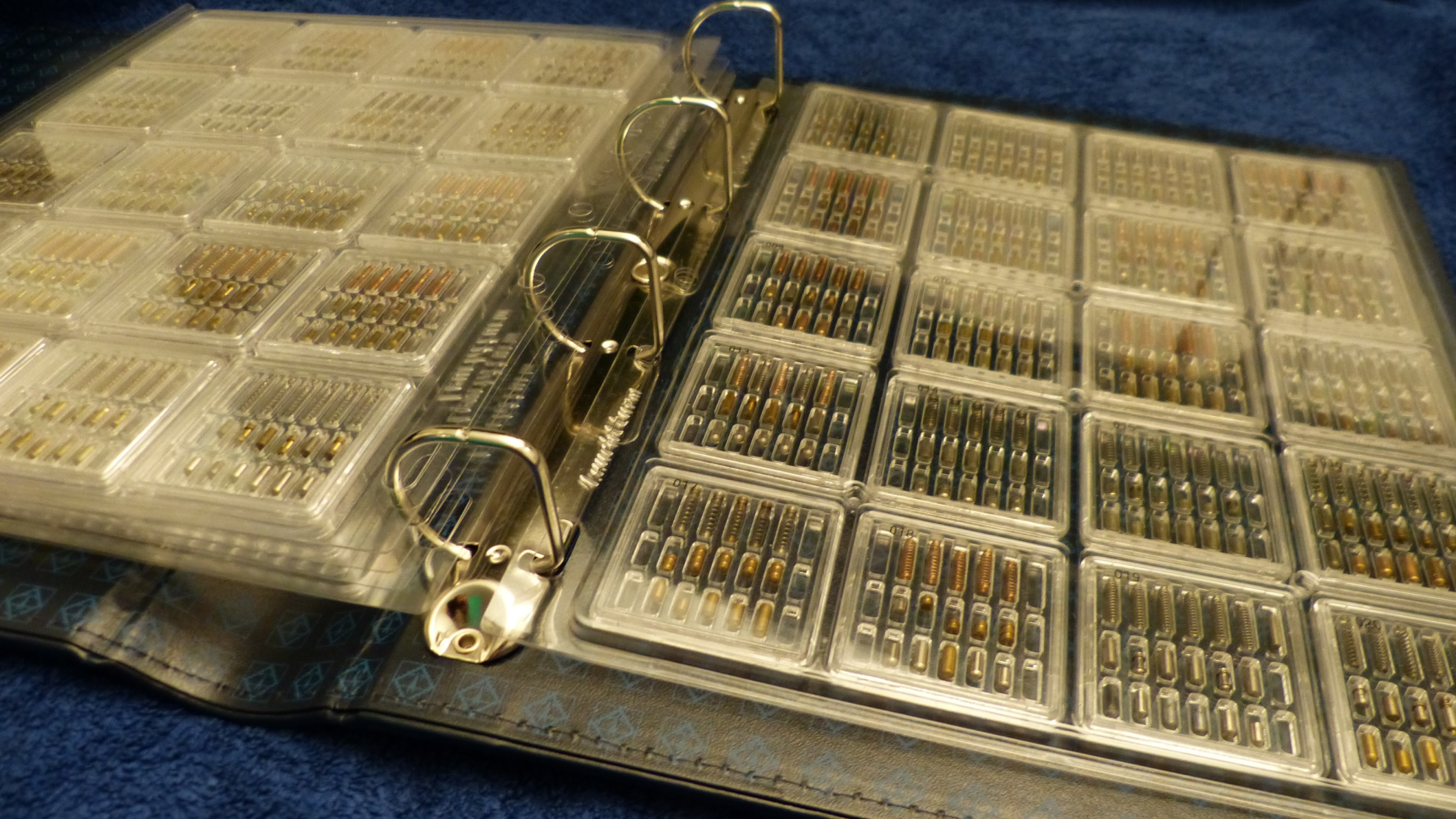
Pin rotation side channel

Distractions:

- Measuring Jig for measuring keys
- Analyzing all locks, all keys, all pins










ROSENGRENS SWEDEN
32A 81
ROSENGRENS SWEDEN



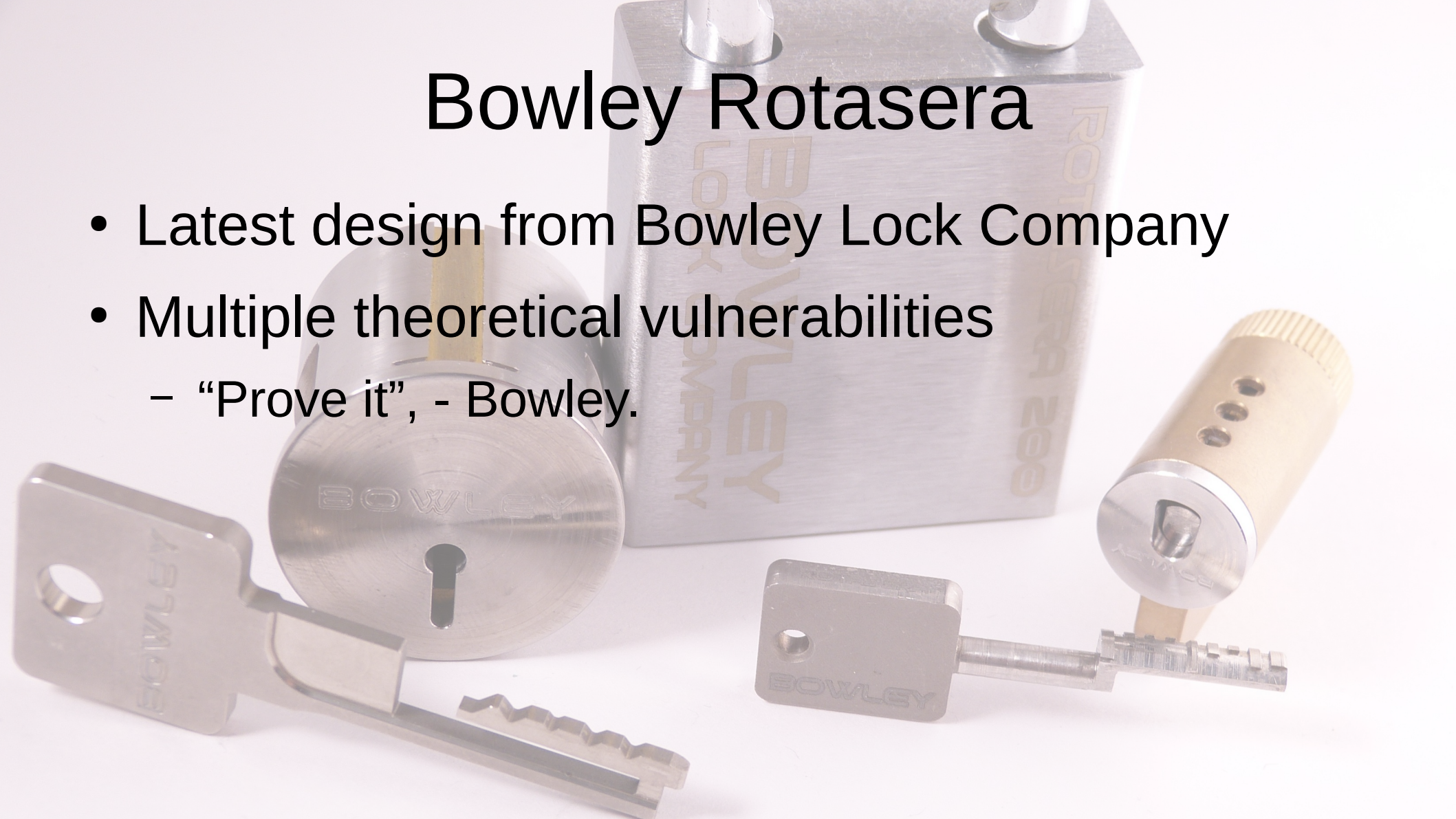

INSEA

Bowley Rotasera



Bowley Rotasera

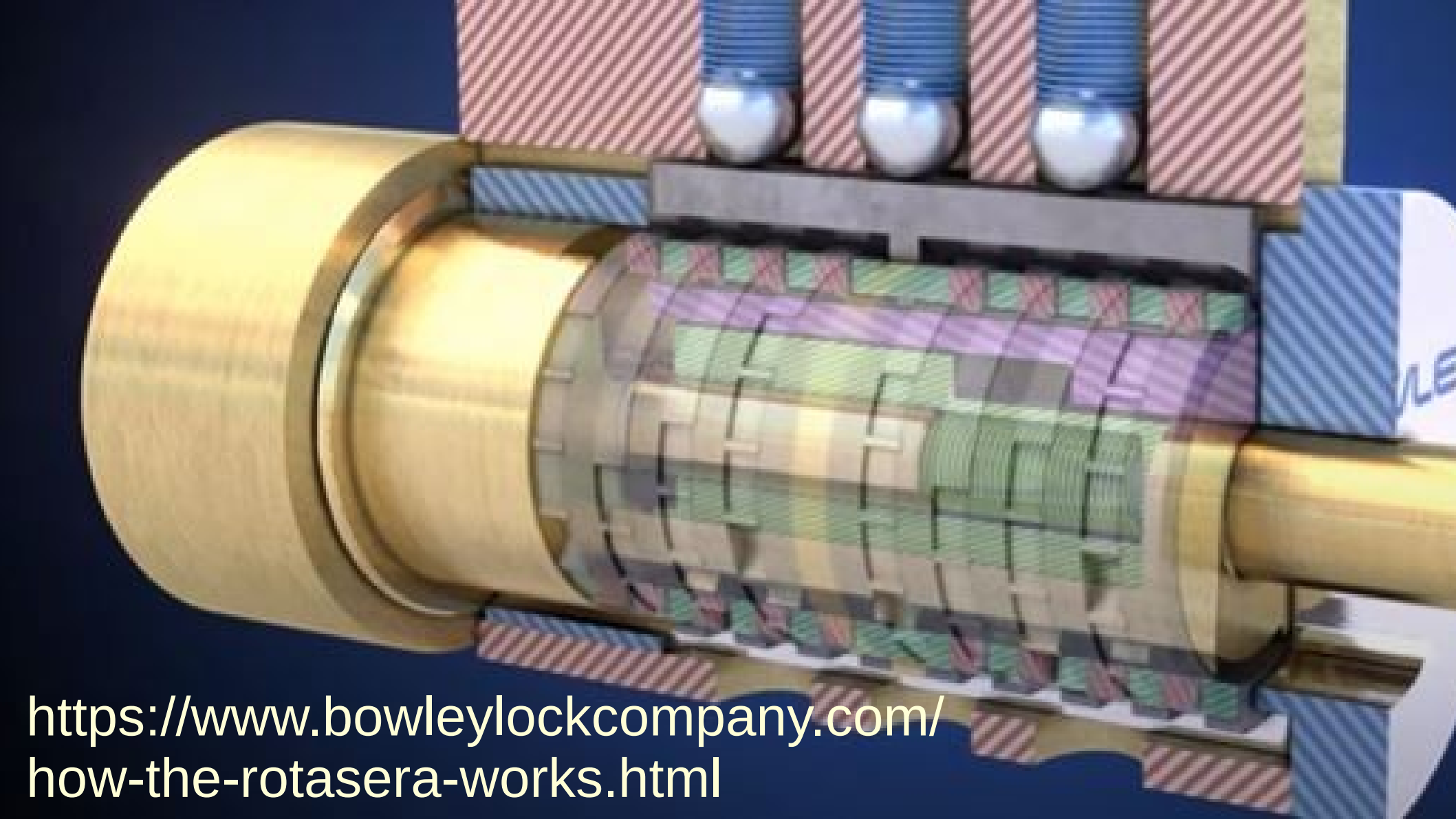
- Latest design from Bowley Lock Company
- Multiple theoretical vulnerabilities
  - “Prove it”, - Bowley.



Bowley Rotasera

- BOWLEY PICKING & GUT (133),
  - **Chris Ahrens**
- Defeating the Bowley, Forever Lock and Yuema 750 - **Mitch ‘Priyer’ Robert**

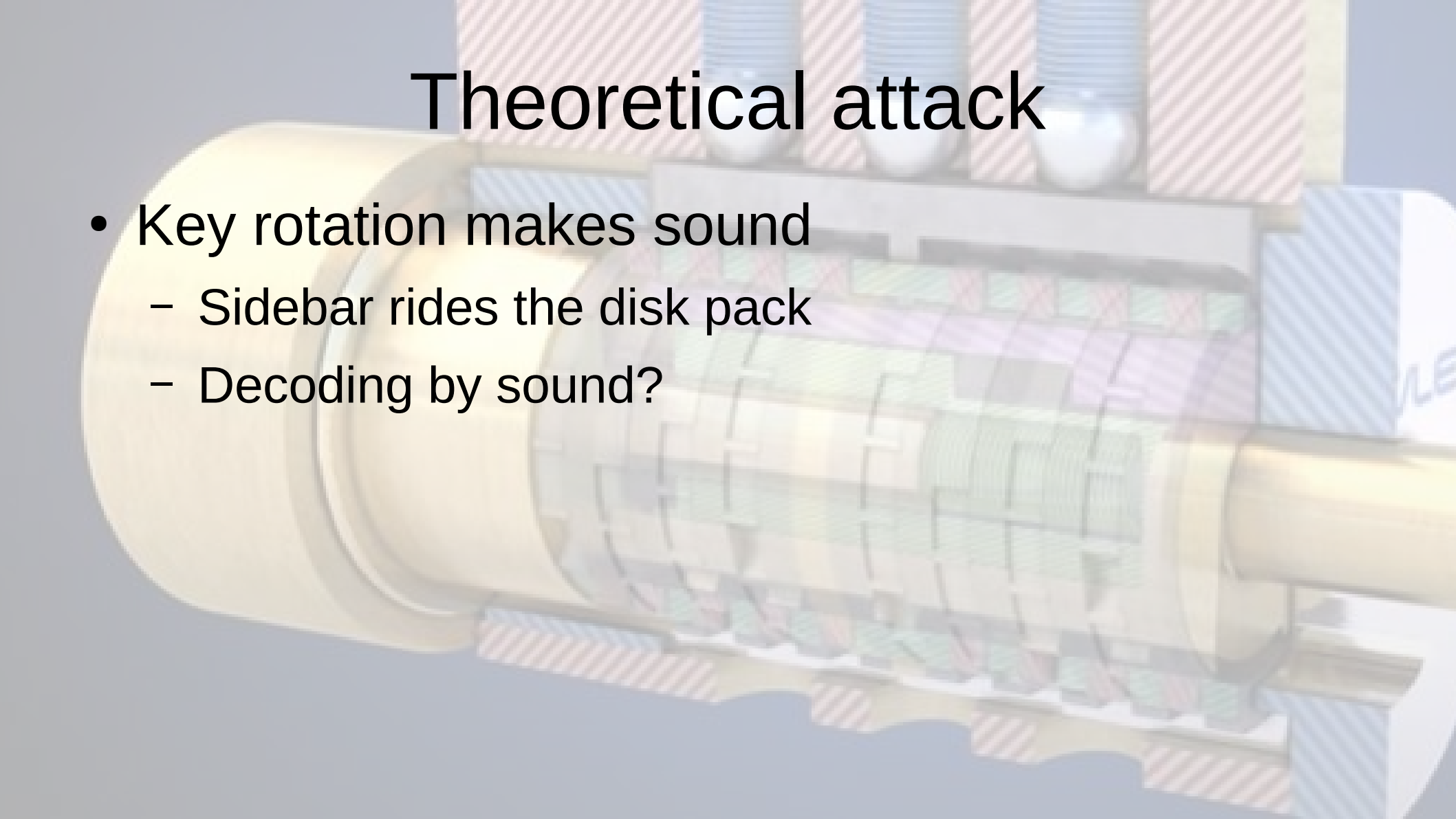




https://www.bowleylockcompany.com/how-the-rotasera-works.html

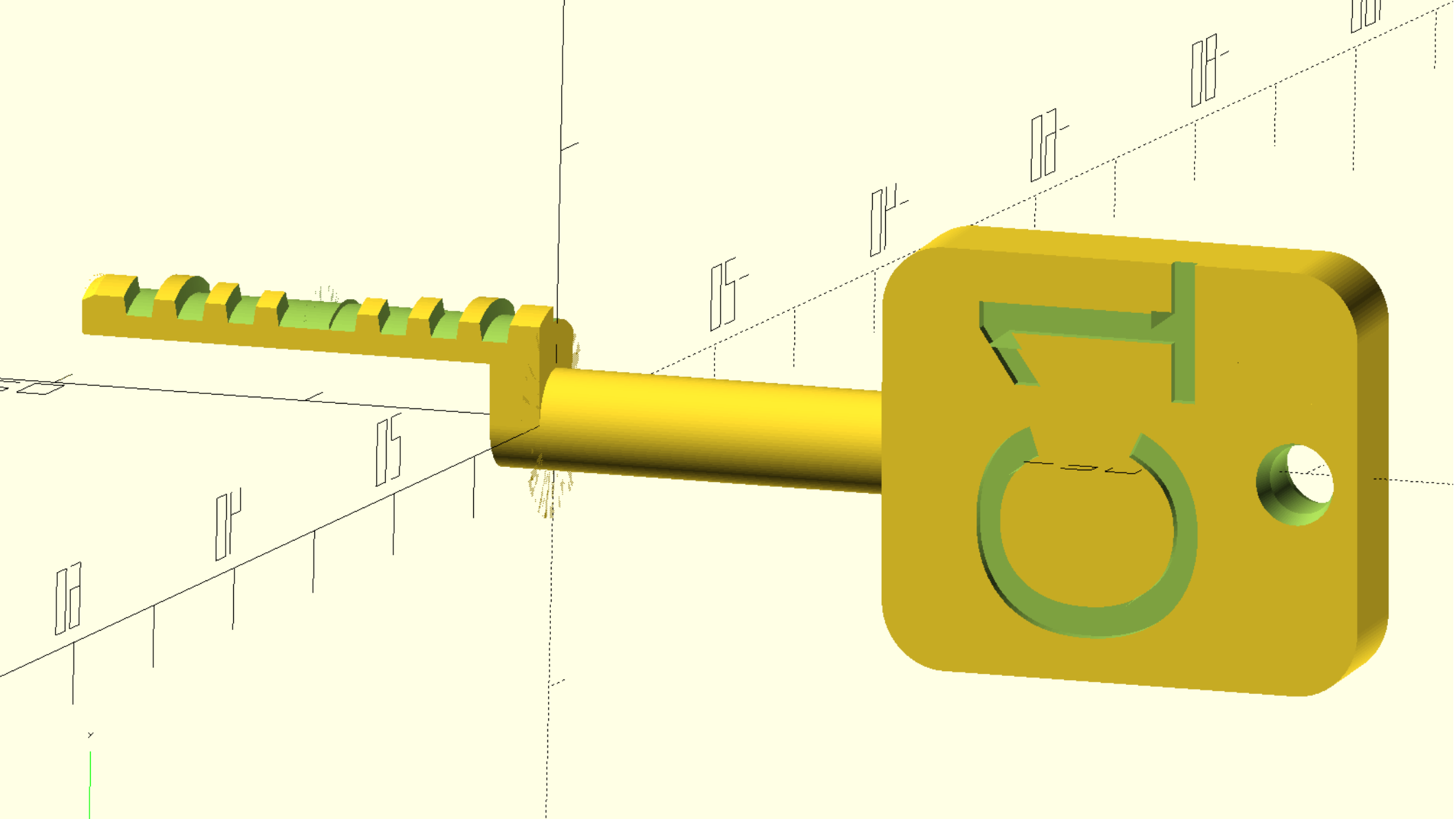
Theoretical attack

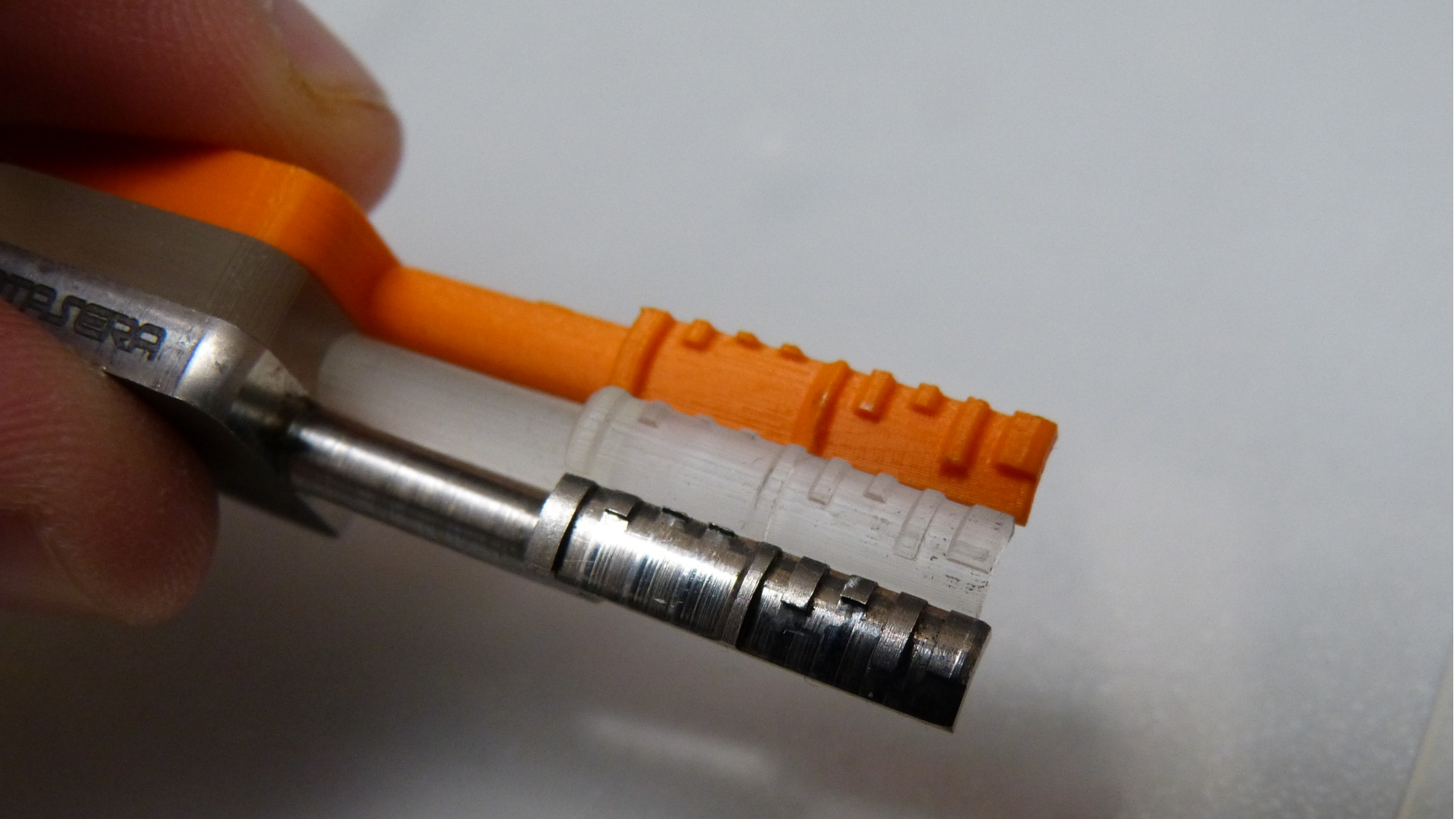
- Key rotation makes sound
  - Sidebar rides the disk pack
  - Decoding by sound?

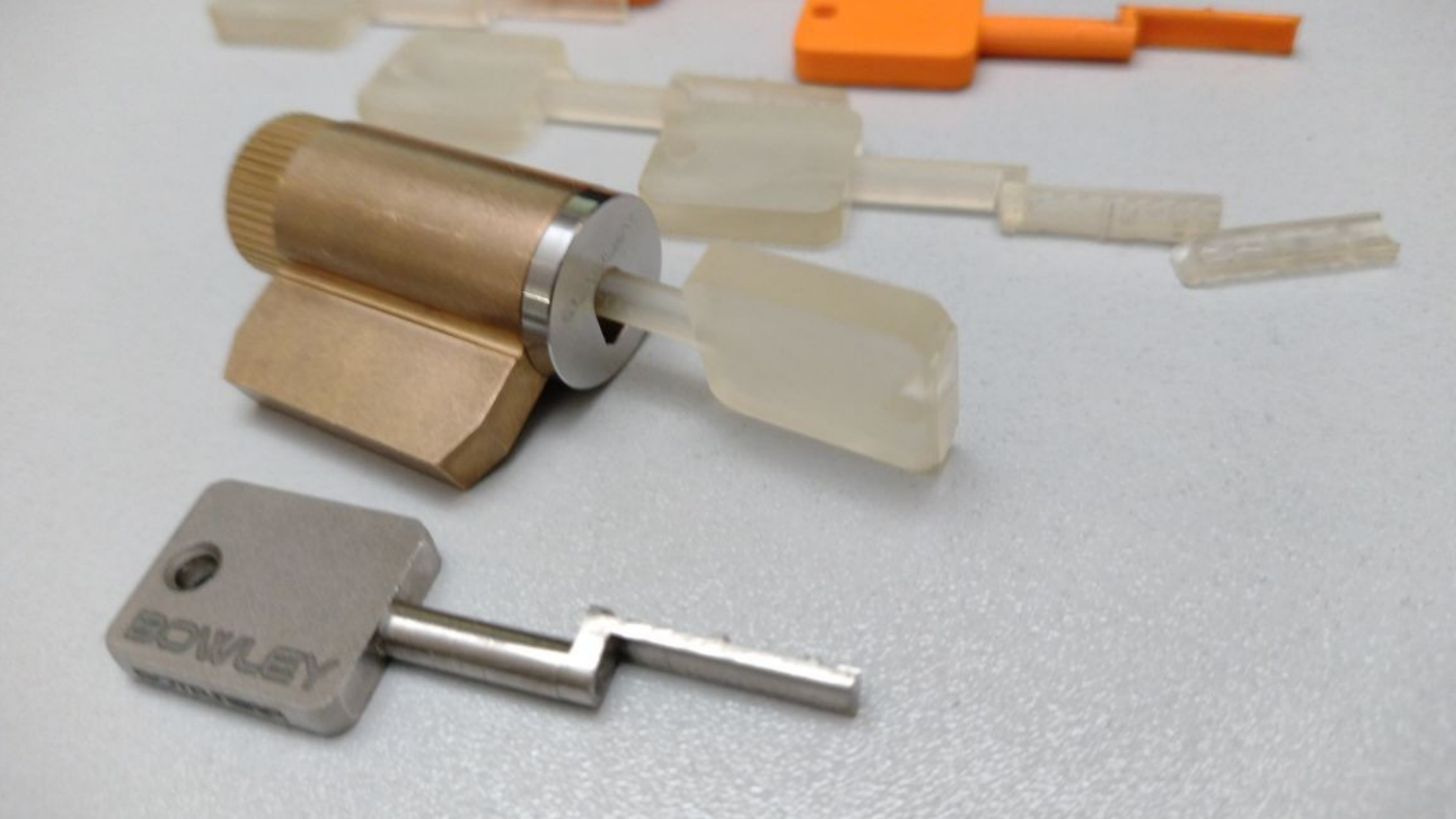


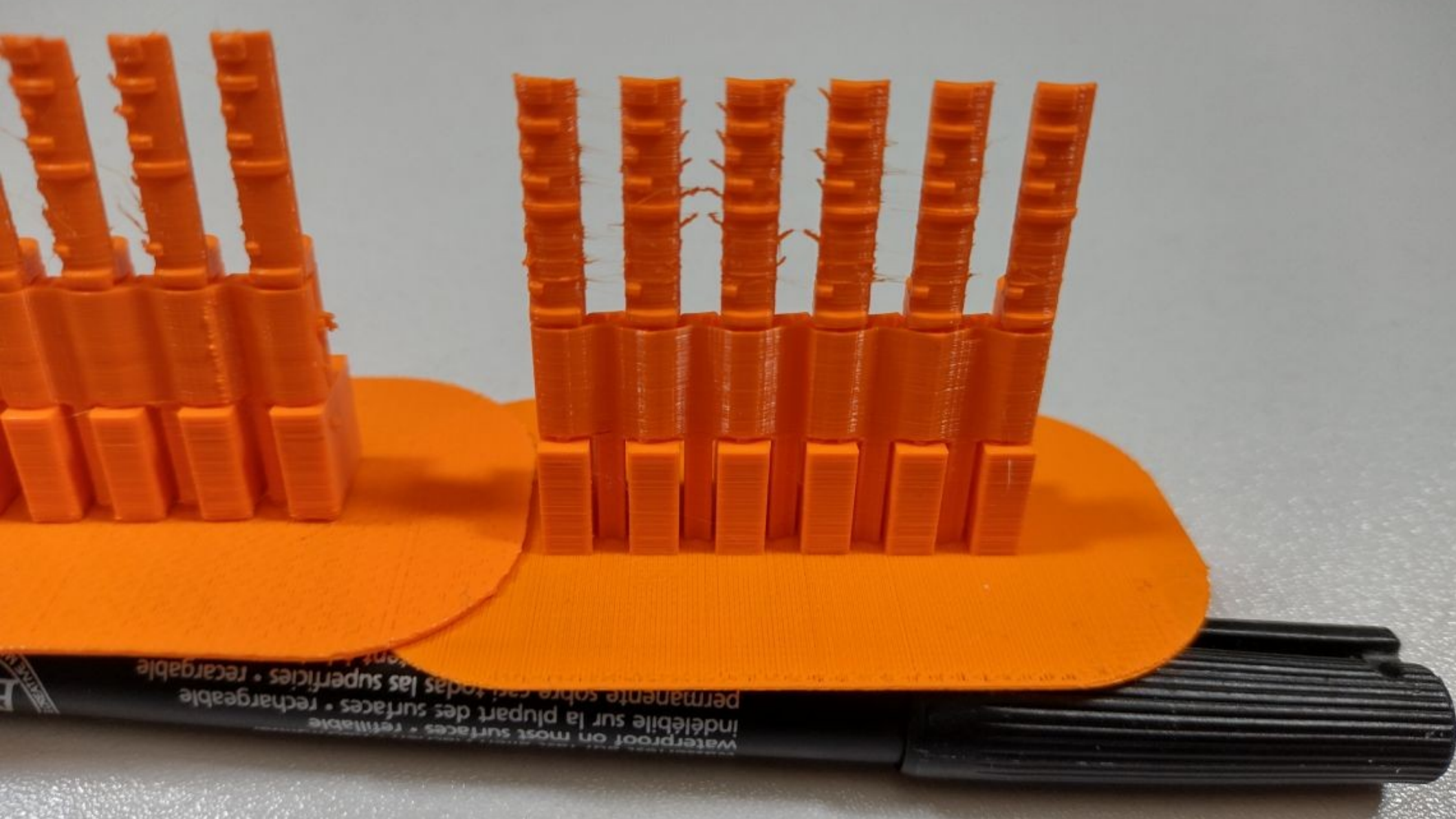

BOWLEY
BOWLEY
ROTASTER





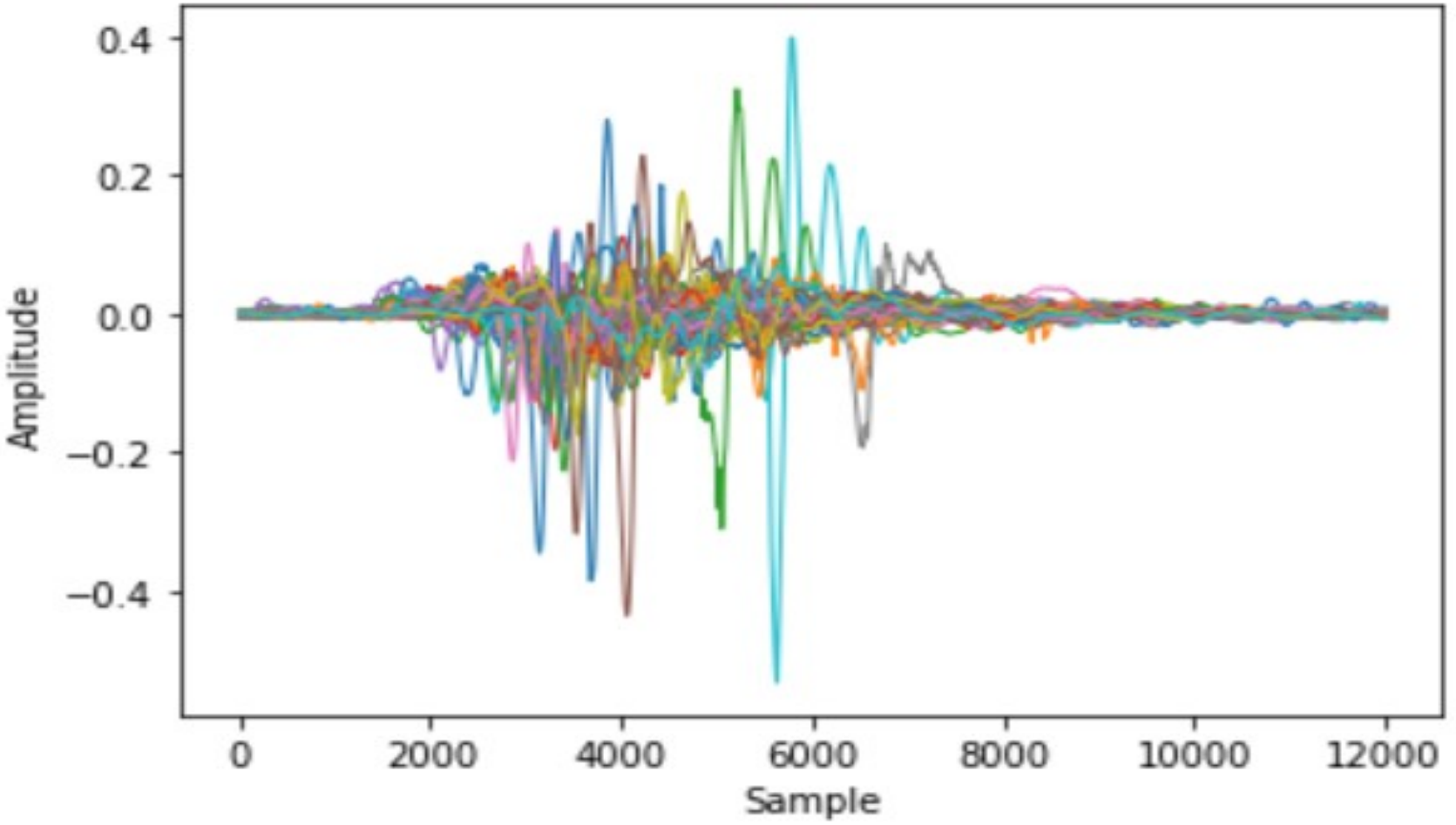



BOWLEY


waterproof on most surfaces • refillable
indélébile sur la plupart des surfaces • rechargeable
permanente sobre casi todas las superficies • recargable


62
5
3

absorbent


0.4
0.2
0.0
−0.2
−0.4
Amplitude
0
2000
4000
6000
8000
10000
12000
Sample

Theoretical attack

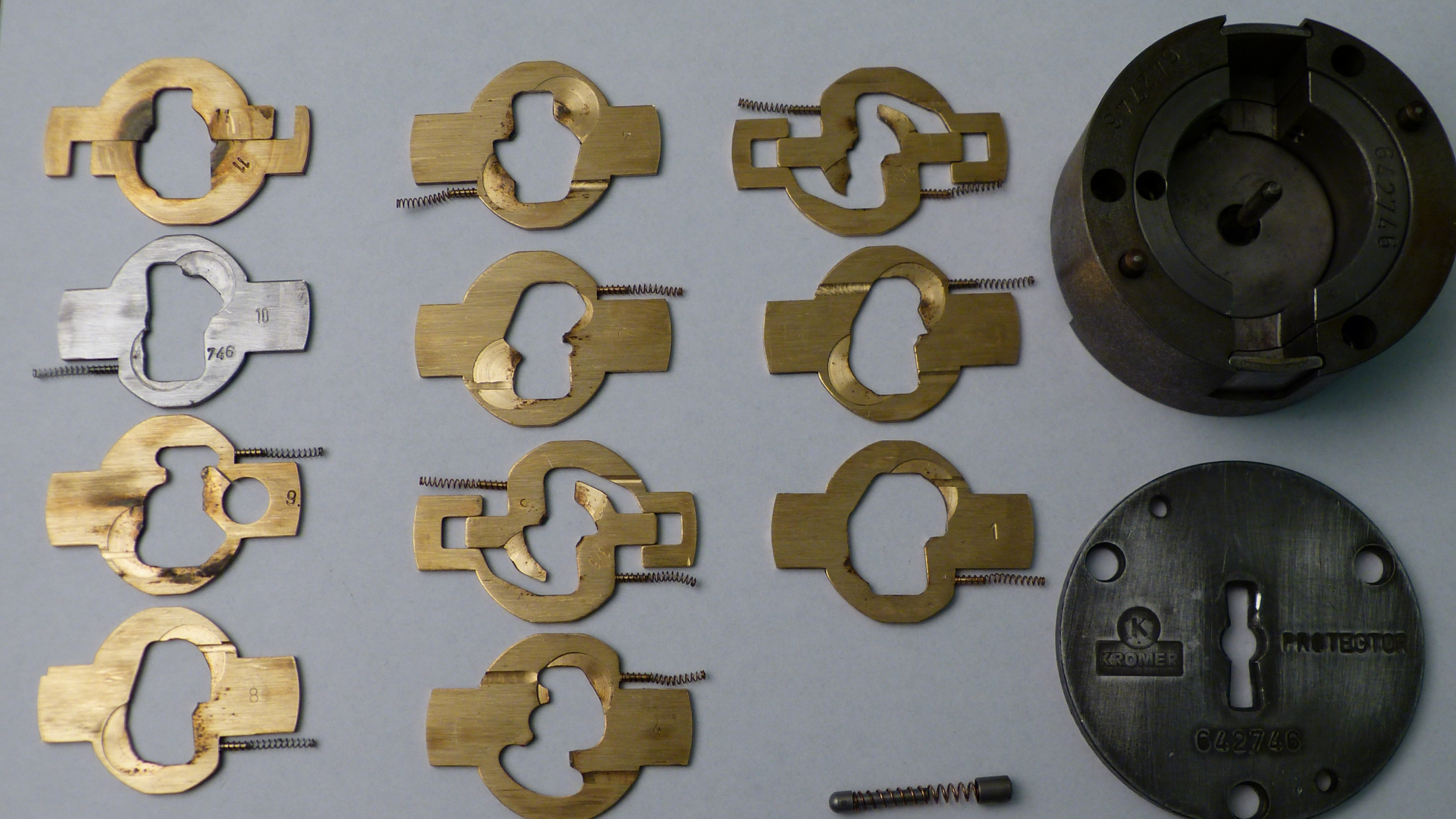
- Decoding by sound?
  - Inconclusive
  - more research needed

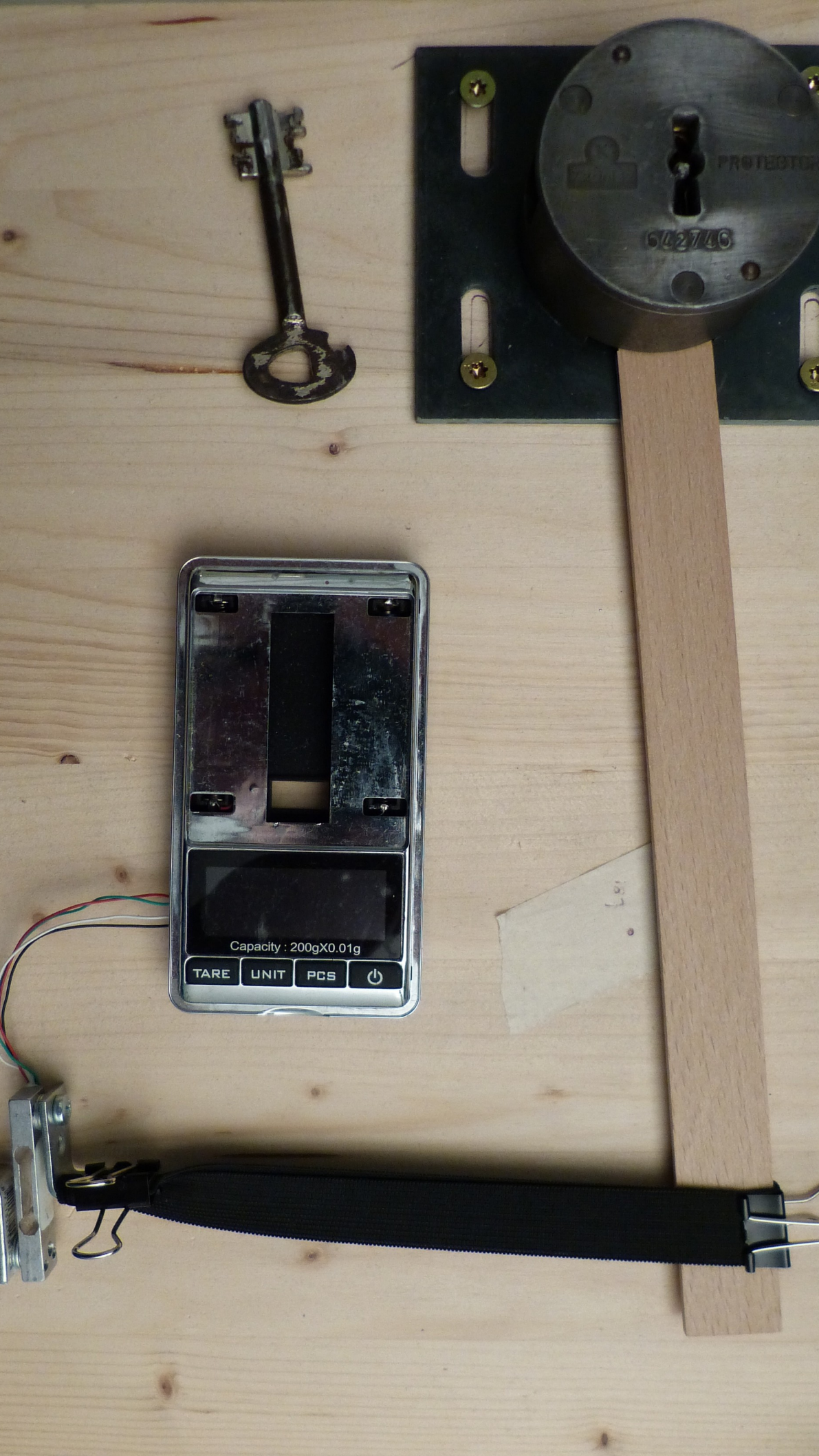
Kromer Protector 2040

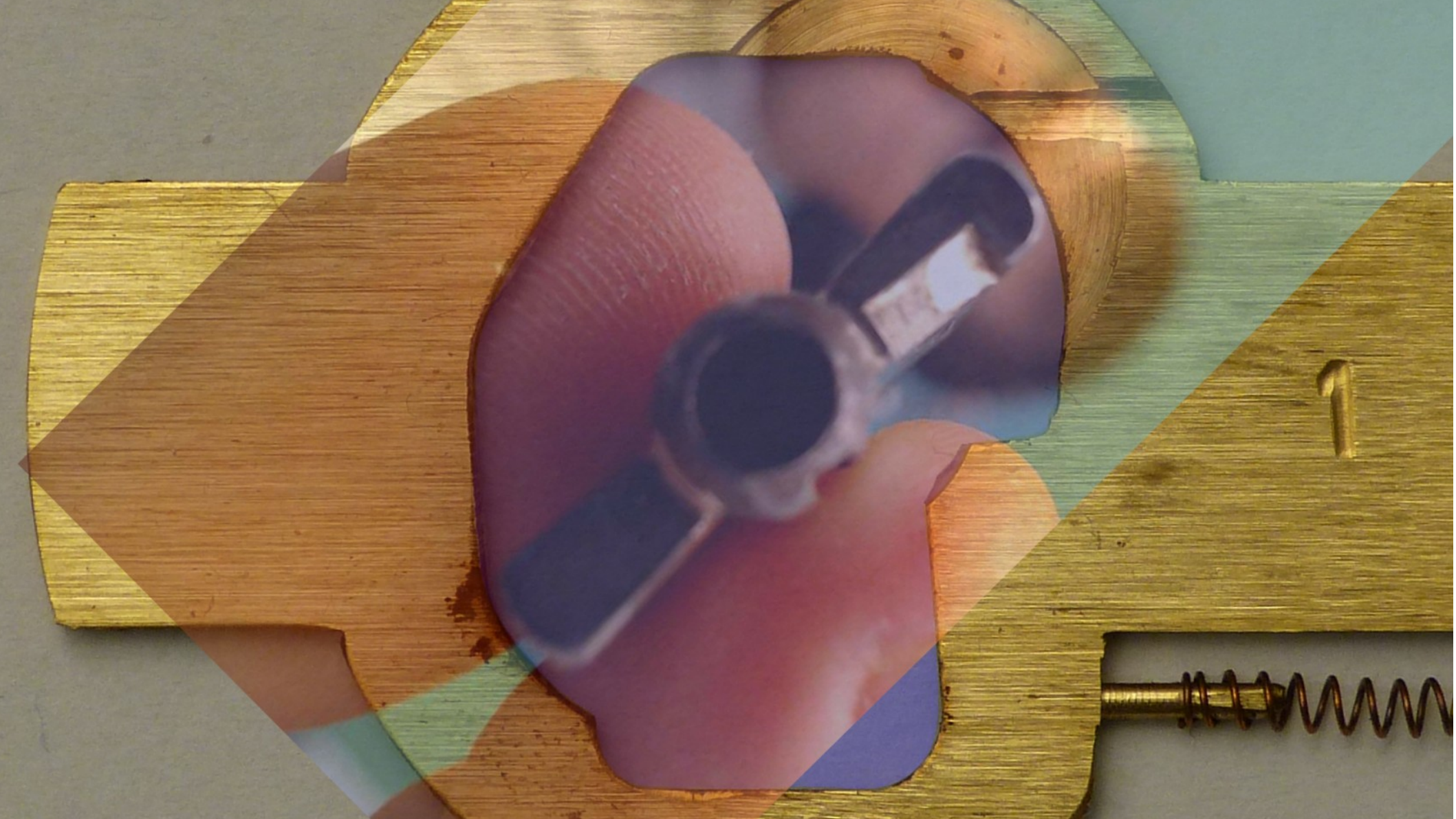


Kromer Protector 2040

- The Unpickable Kromer Protector - **Jaakko Fagerlund** - OzSecCon 2019
- DEF CON Safe Mode Lock Picking Village - **Zeefeene** - High Security Wafer Locks An Oxymoron
- Kromer Protector (Patent-Post-Kassetten-Eingerichte) Picked and Gutted - **WestLockPicking**


10
746
9
8
7
1
642746
K
KROMER
PROTECTOR
642746


PROTECTOR
642746
Capacity : 200gX0.01g
TARE
UNIT
PCS

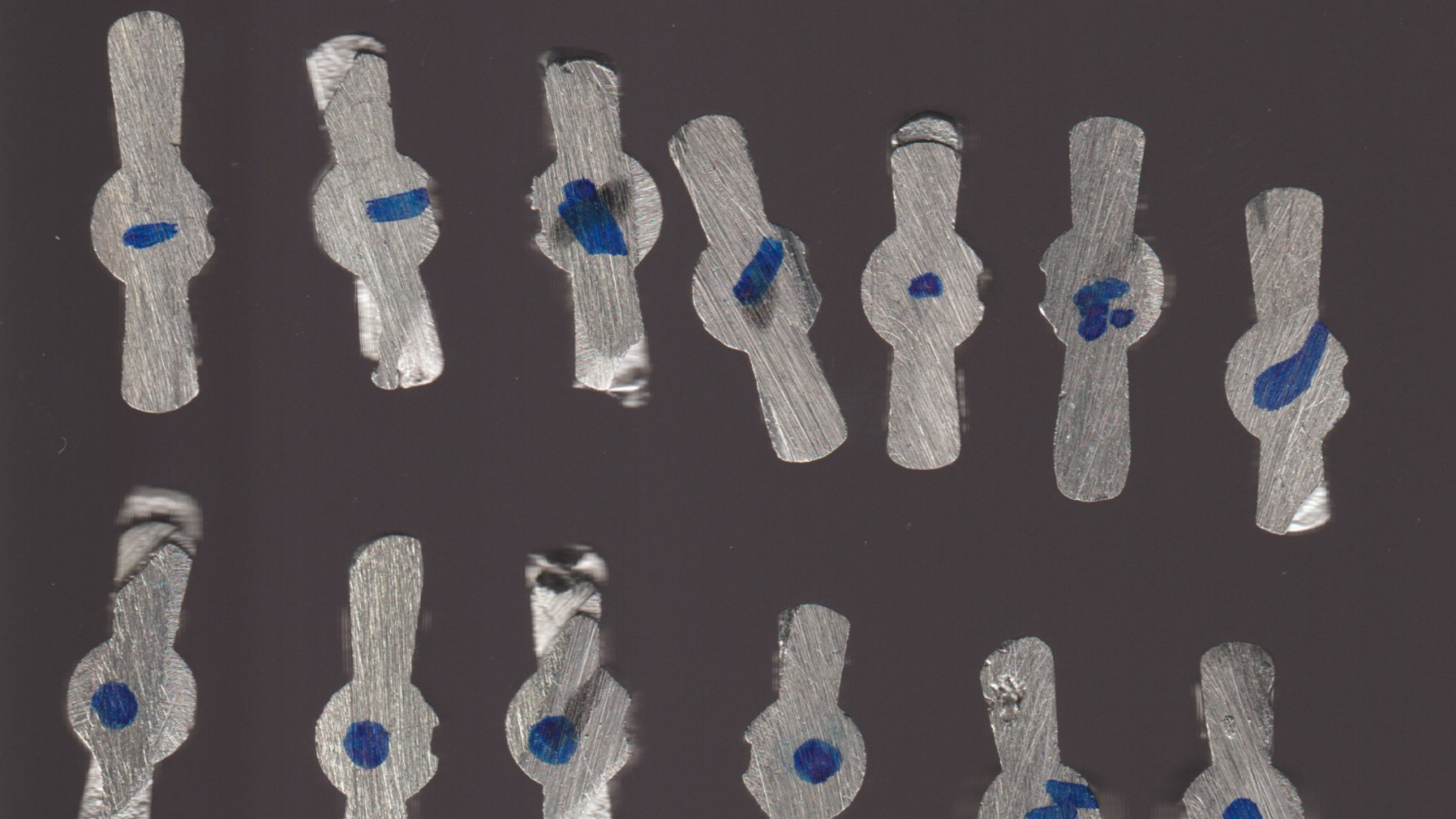


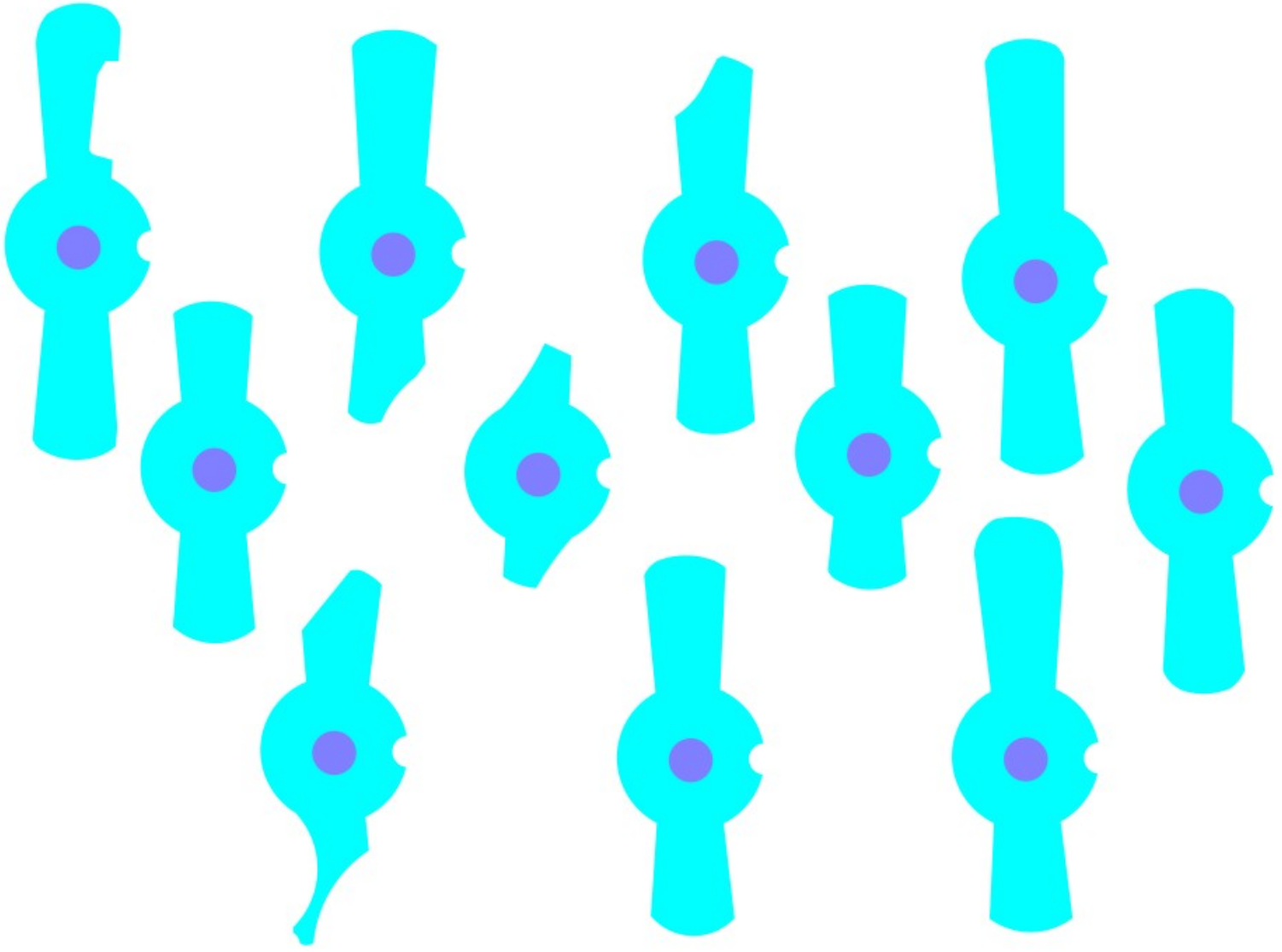


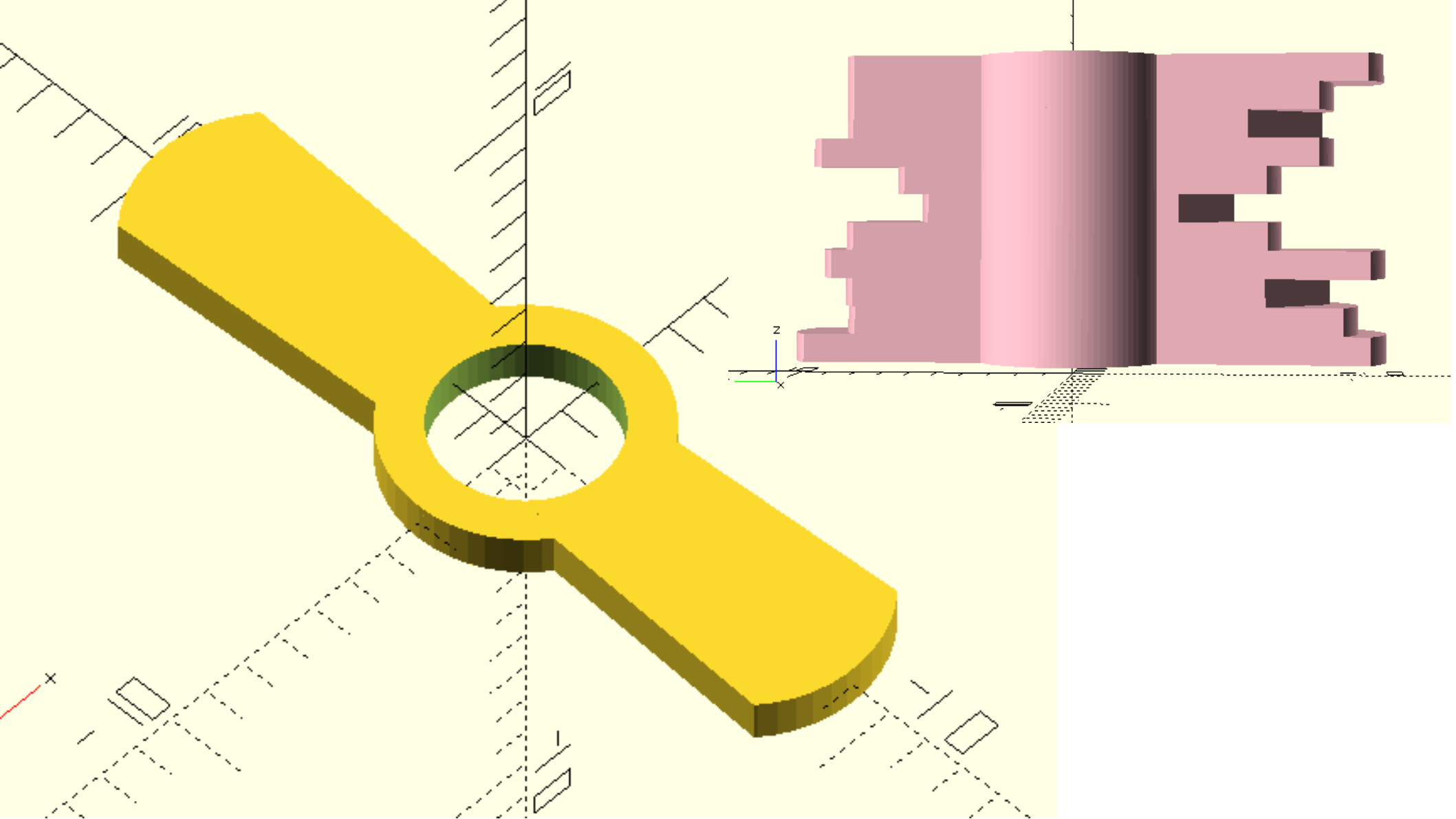











z
x



Kromer_base_v2.scad - OpenSCAD

File Edit Design View Help

Editor

```
    rotate([0,0,-45]) translate([d,0,0]) circle((s)/2);
    rotate([0,0,0]) translate([d,0,0]) circle((s)/2);
    mirror([1,0,0]){
        rotate([0,0,45]) translate([d,0,0]) circle((s)/2);
        rotate([0,0,-45]) translate([d,0,0]) circle((s)/2);
        rotate([0,0,0]) translate([d,0,0]) circle((s)/2);
        }
}

module ring(){
    difference(){
        //base
        union(){
            color( "RoyalBlue", 0.15 )difference(){
                circle(68/2);
                circle(49.2/2);
                holes((68+49)/4,2);
            }

            //core
            color( "DarkOrange", 0.50 )difference(){
                circle((49.2-0.3)/2);
                circle((36.6+0.3)/2);
                holes((49+36)/4,2);
            }
        }
        square([14.2+0.50, 68],true);
    }
    //square([14.2+0.40, 68],true);
}

module base(){
    color( "RoyalBlue", 0.15 )difference(){
        circle(68/2);
        circle(49.2/2);
        square([14.2+0.50, 68],true);
        holes((68+49)/4,2);
    }
    color( "DarkOrange", 0.50 )difference(){
        circle((49.2-0.3)/2);
        circle(1.05);
        holes((49+36)/4,2);
    }
}

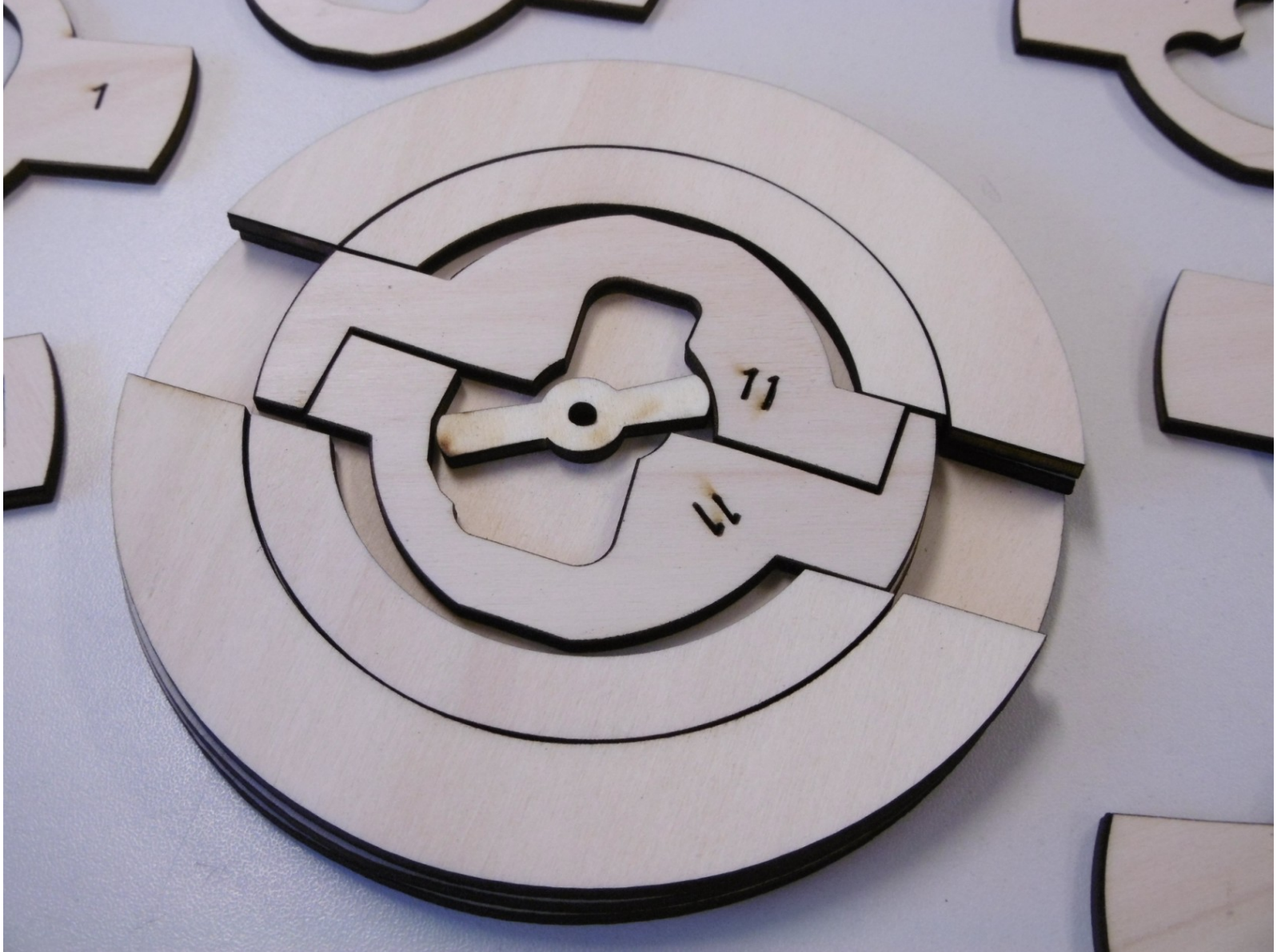
module bottom(){
    {
        color( "RoyalBlue", 0.15 ) difference(){
```

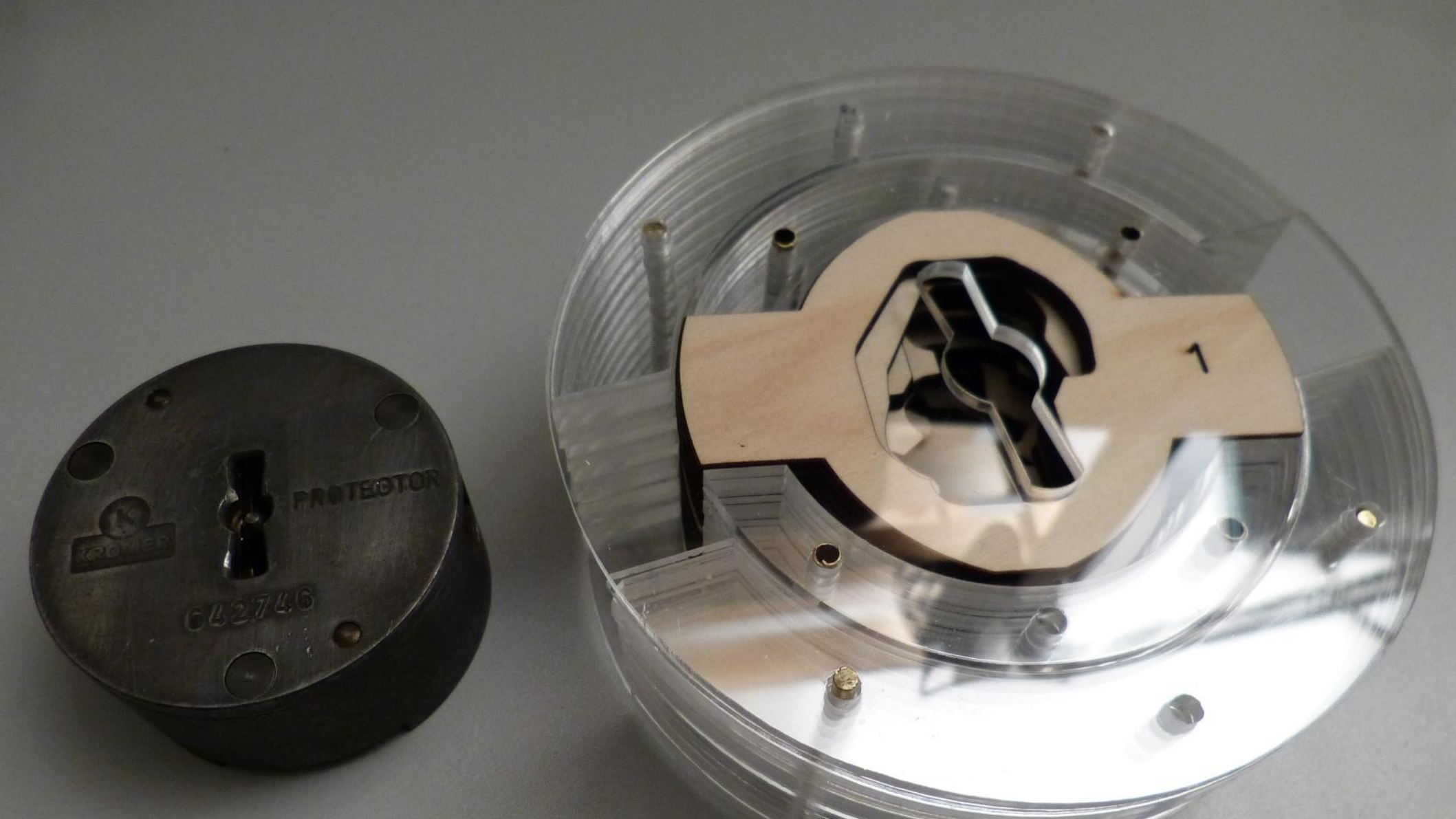
Console

```
Loaded design 'E:/Doc/Dropbox/lock/Kromer/Blackbag1/Kromer_base_v2.scad'.
Compiling design (CSG Tree generation)...
Compiling design (CSG Products generation)...
Geometries in cache: 14
Geometry cache size in bytes: 13664
CGAL Polyhedrons in cache: 0
CGAL cache size in bytes: 0
Compiling design (CSG Products normalization)...
Normalized CSG tree has 481 elements
Compile and preview finished.
Total rendering time: 0 hours, 0 minutes, 7 seconds
```

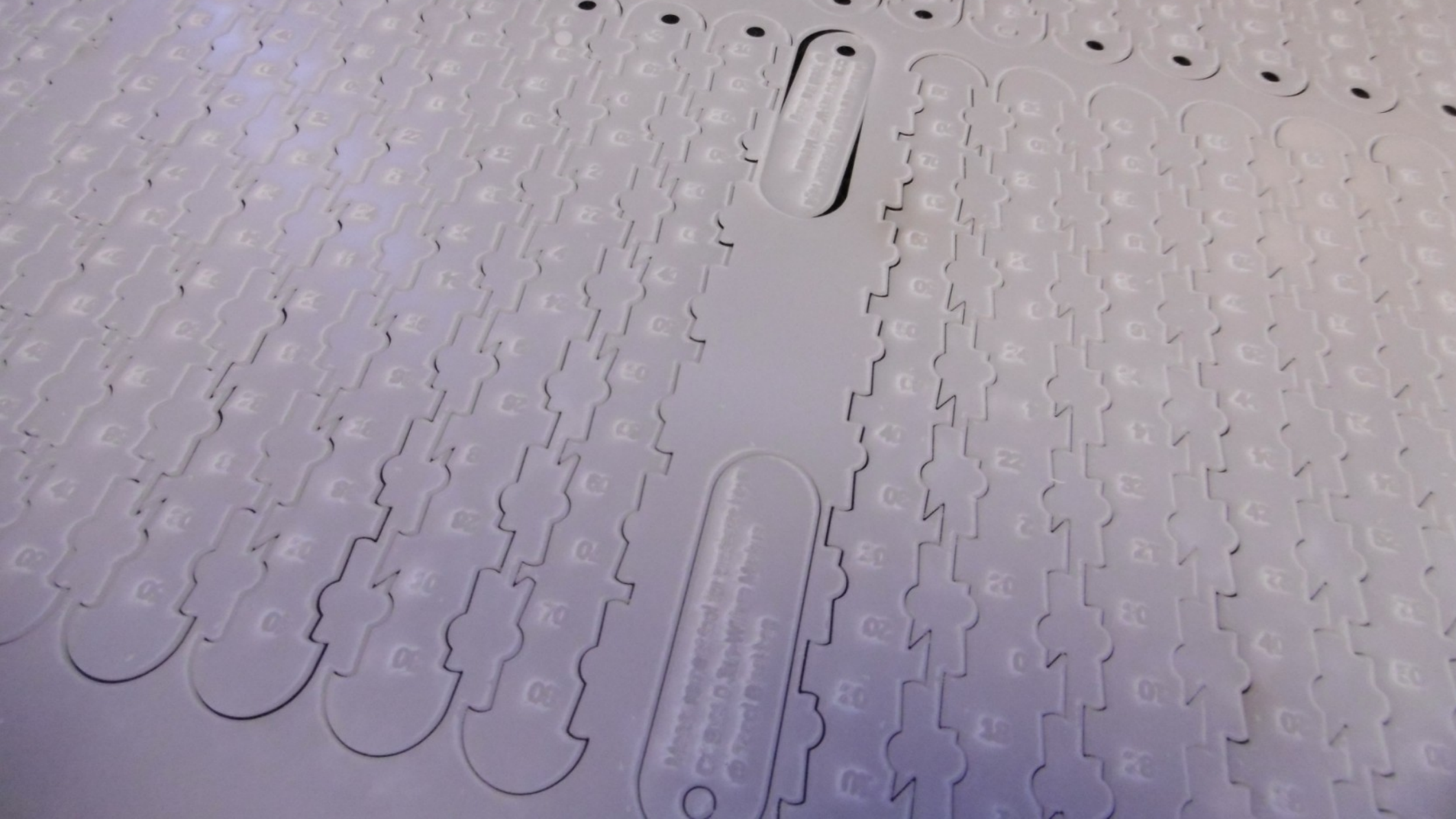
Viewport: translate = [0.28 4.84 12.13], rotate = [45.20 0.00 57.20], distance = 172.84 (1185x724)

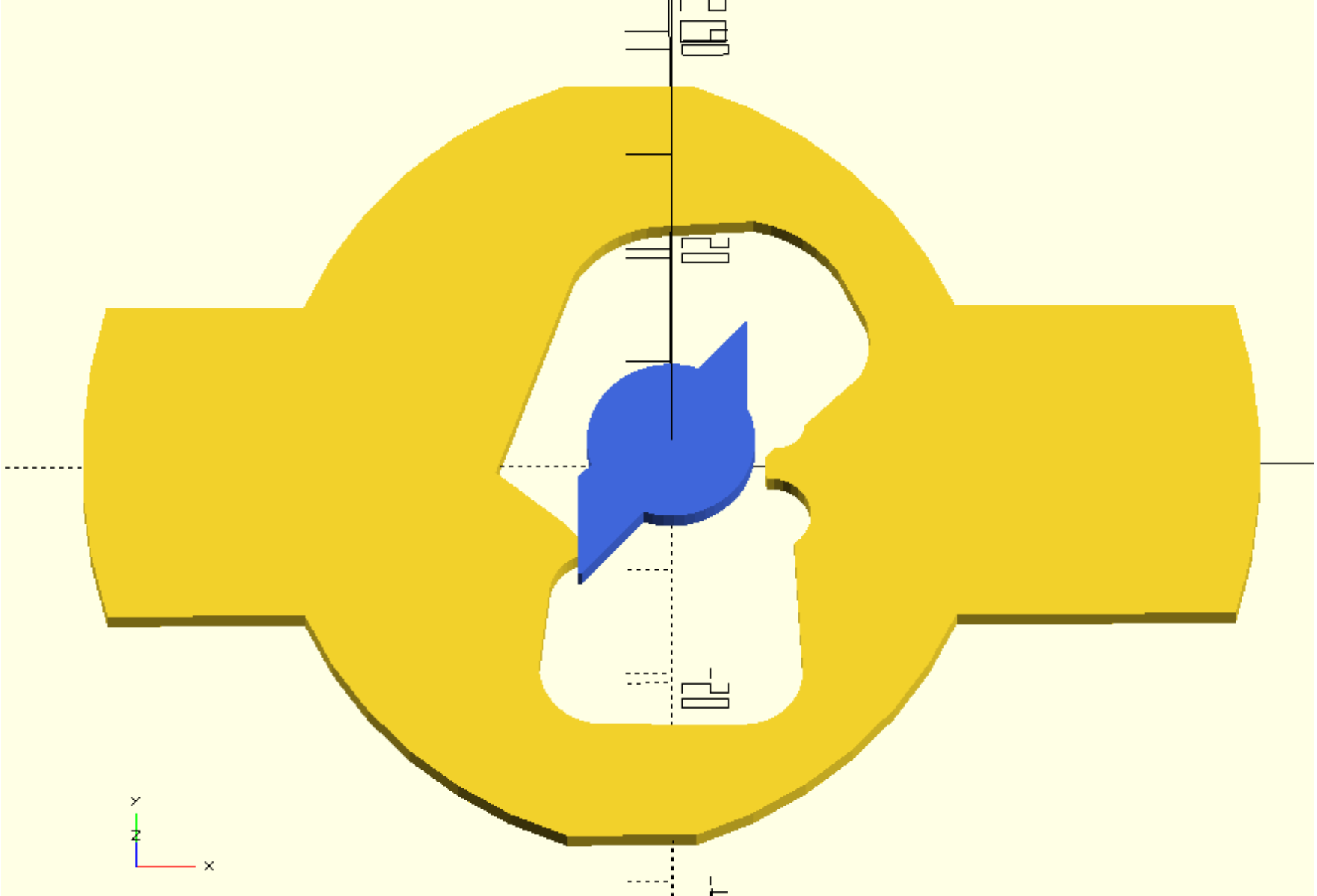
OpenSCAD 2019.05

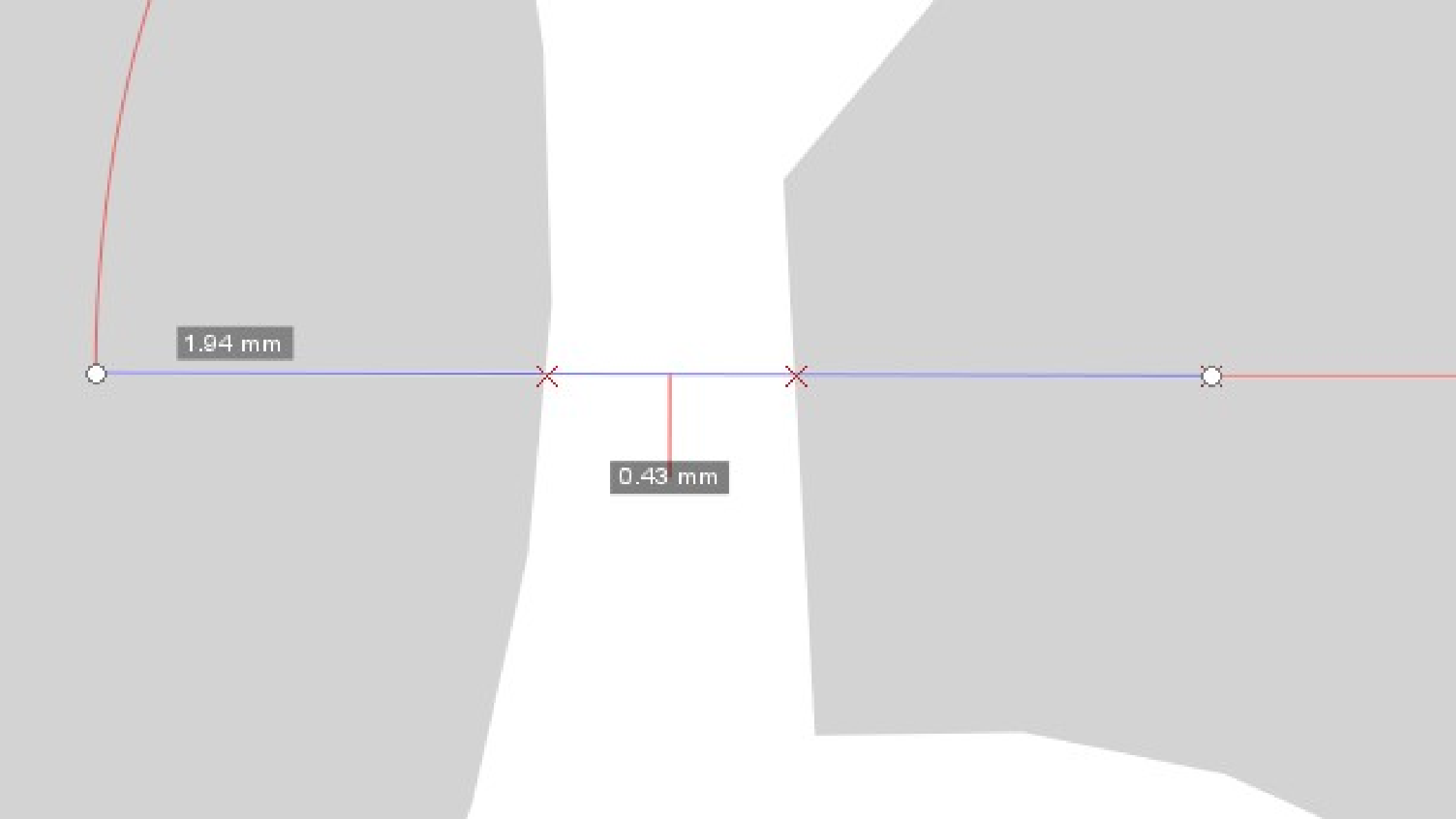

1
11
11

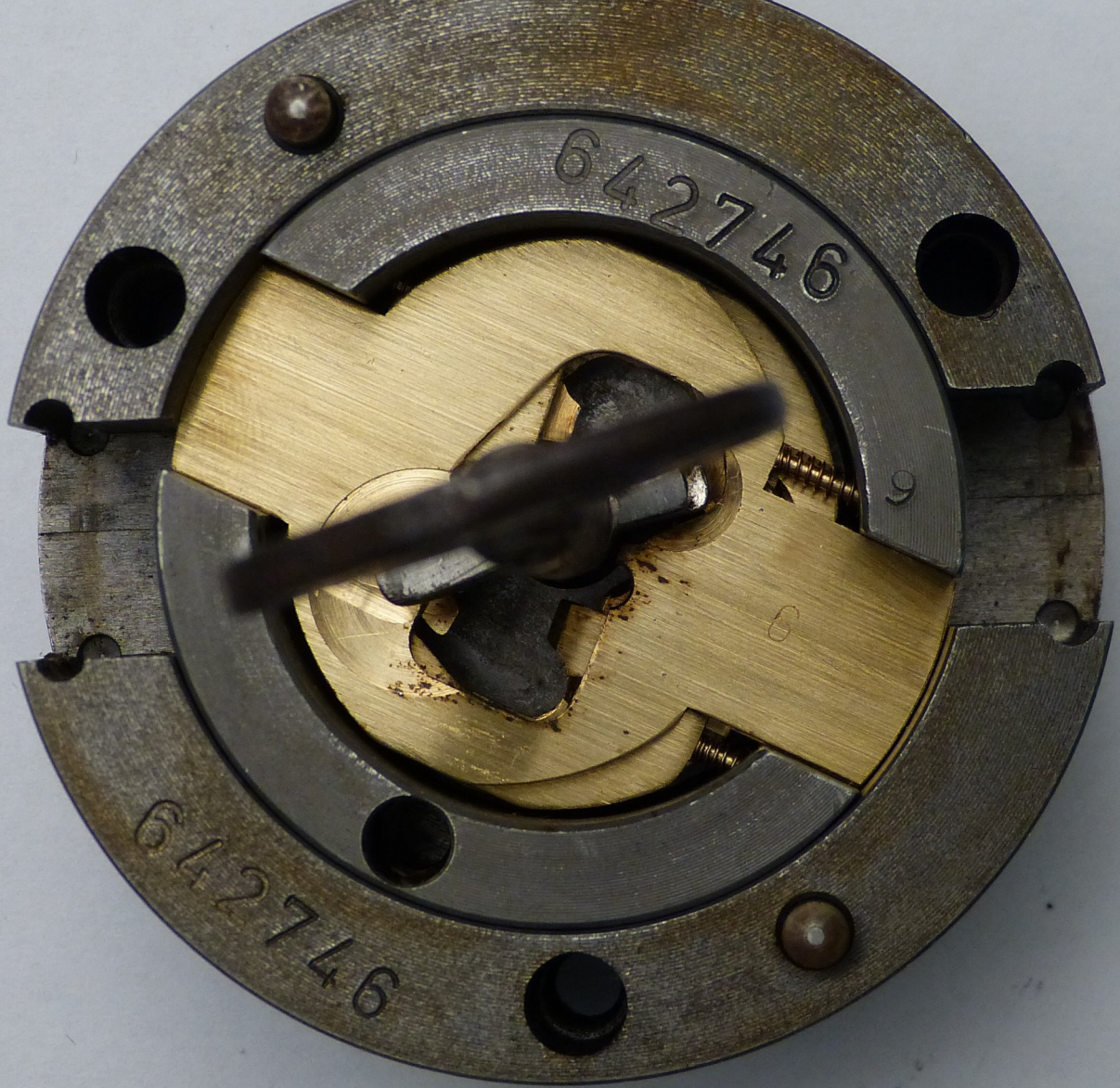

PROTECTOR
642746
1

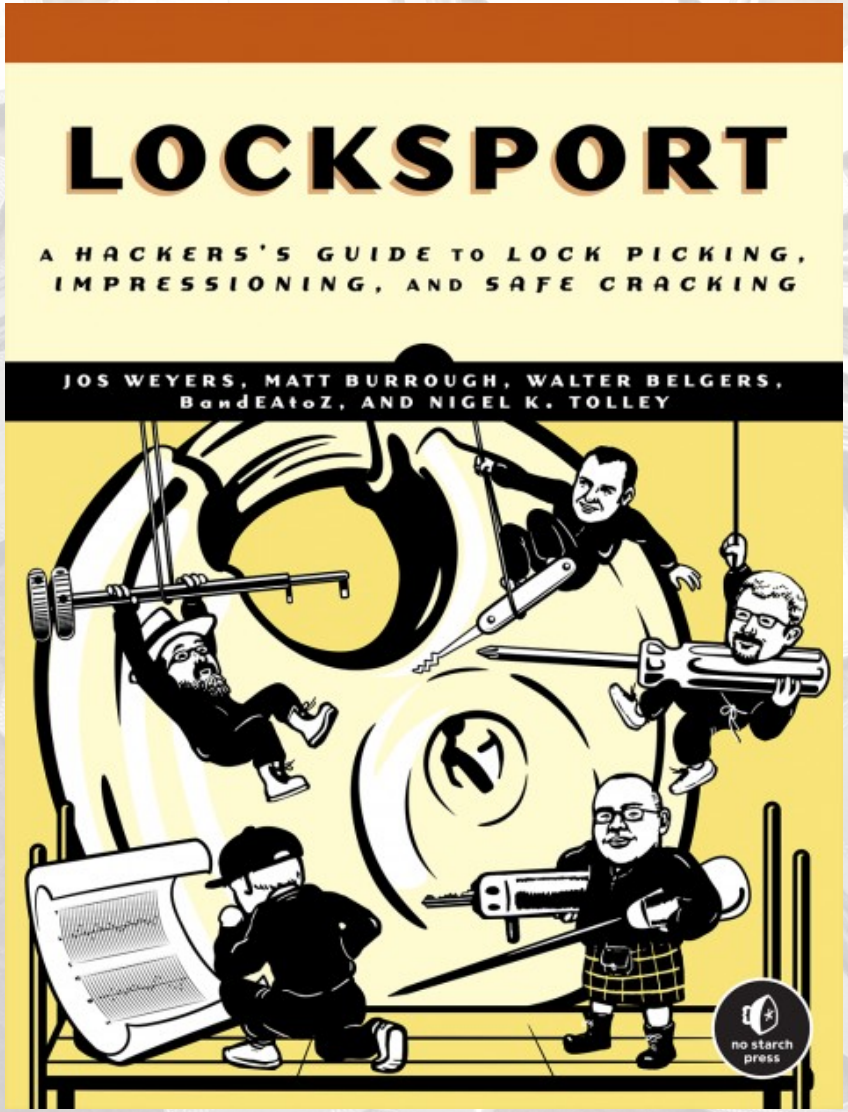
0 20 10 30 20 40 30 50 40 60 50 70 60 80
-1 61 0 20 1 21 2 22 3 23 4 24 5 25
4 24 5 25 6 26 7 27 8 28 9 29 10 30
9 29 10 30 11 31 12 32 13 33 14 34 15 35
14 34 15 35 16 36 17 37 18 38 19 39 20 40
19 39 20 40 21 41 22 42 23 43 24 44 25 45
24 44 25 45 26 46 27 47 28 48 29 49 30 50
29 49 30 50 31 51 32 52 33 53 34 54 35 55
34 54 35 55 36 56 37 57 38 58 39 59 40 60
39 59 40 60 41 61 42 62 43 63 44 64 45 65
44 64 45 65 46 66 47 67 48 68 49 69 50 70
49 69 50 70 51 71 52 72 53 73 54 74 55 75
54 74 55 75 56 76 57 77 58 78 59 79 60 80




Y
Z
X


1.94 mm
0.43 mm


642746
642746


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?
  - 3rd & final Impressioning workshop later today

- Contact:

Jan-willem@Toool.nl

@jwrm22