DEF CON 26

2018-08-10



Attacking the Knox Box and Other Keyed Alike Systems

m010ch_

?


SECURITY
UL
LISTED
EQUIPMENT
CE
MDL3200 SERIES
SN 32-518464
OUTDOOR USE
THE KNOX COMPANY, PHOENIX, AZ

@m010ch_





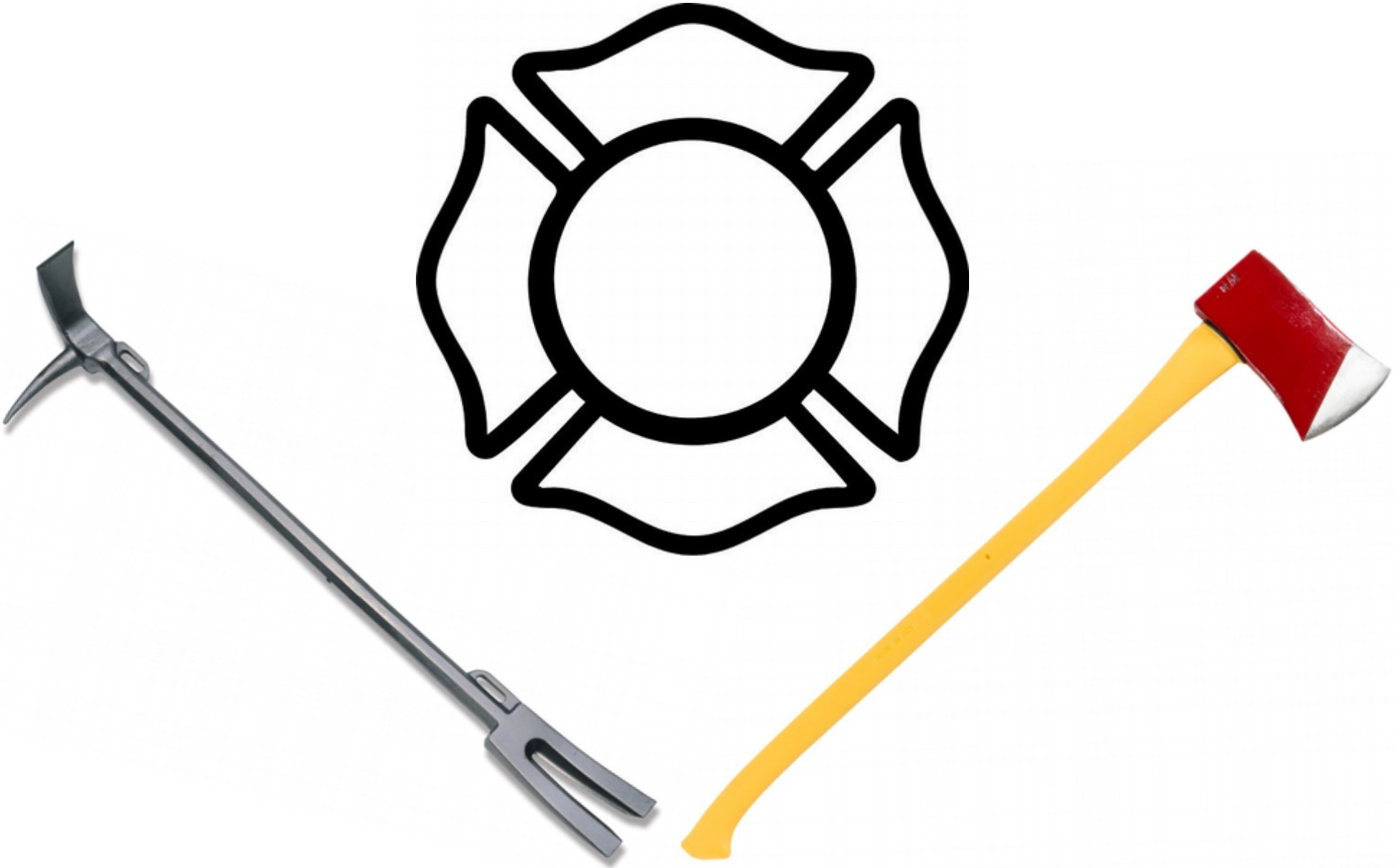


zamak@protonmail.ch

Key boxes


SECURITY
LISTED
SN 32-518464
OUTDOOR USE
THE KNOX COMPANY, PHOENIX, AZ

Key boxes



Key boxes



Key boxes



Who makes them?



Knox Boxes


FIRE DEPARTMENT
KNOX
LIFE SAFETY
SYSTEM
FIRE & RESCUE ENTRY
DO NOT REMOVE
MODEL 3200
SERIAL #
THE KNOX COMPANY, PHOENIX, AZ

Knox Boxes


FIRE DEPARTMENT
KNOX
LIFE SAFETY
SYSTEM
FOR RESCUE ENTRY
DO NOT REMOVE
4400 SERIES
OUTDOOR USE

Knox Boxes

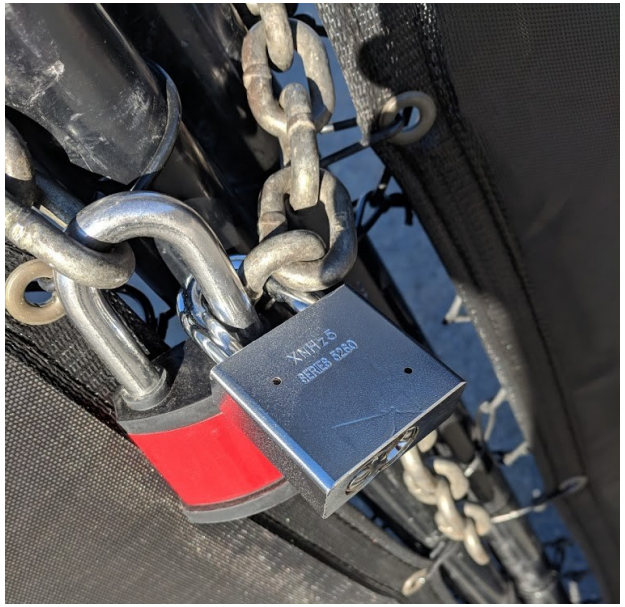




Knox Boxes

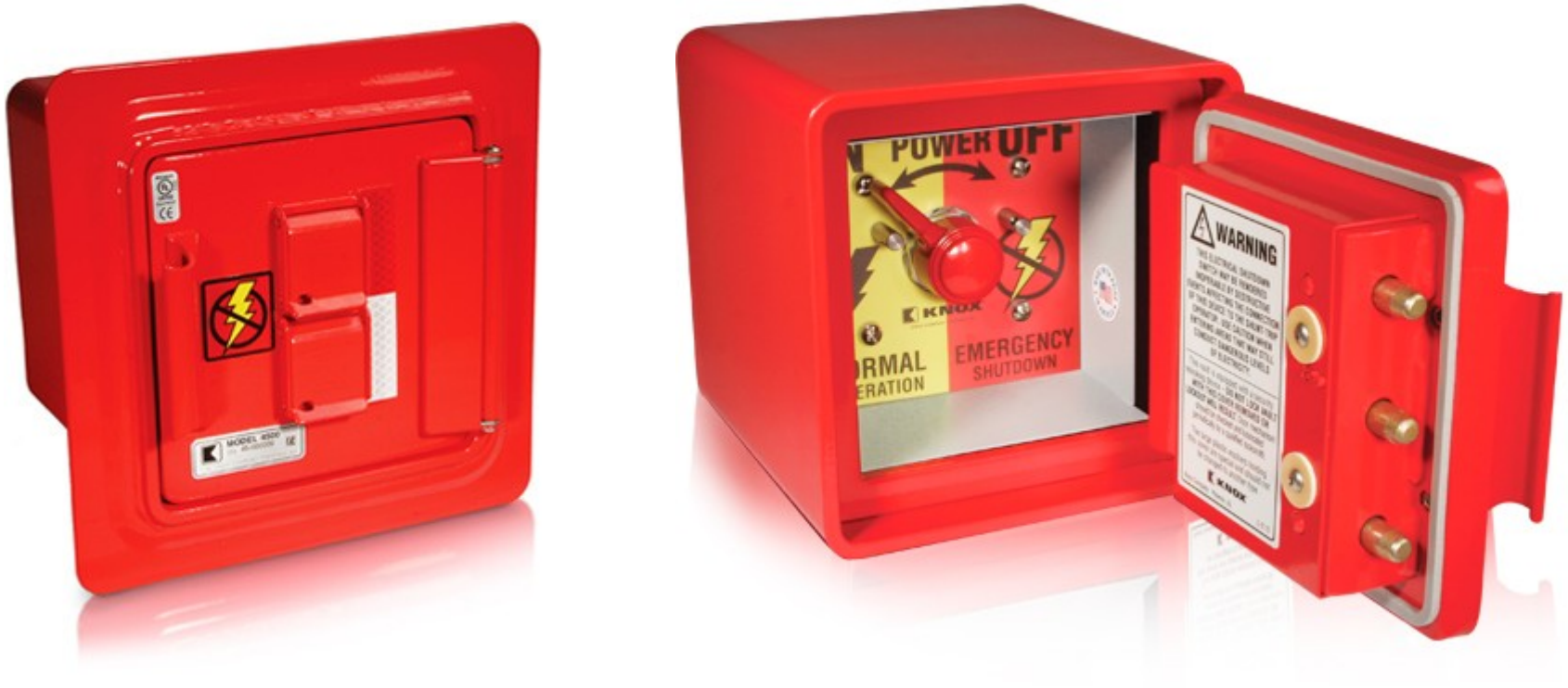

FIRE DEPT


FIRE DEPT.
KNOX
3772
FIRE DEPT.
KNOX
3770
FIRE DEPT.
KNOX
3771

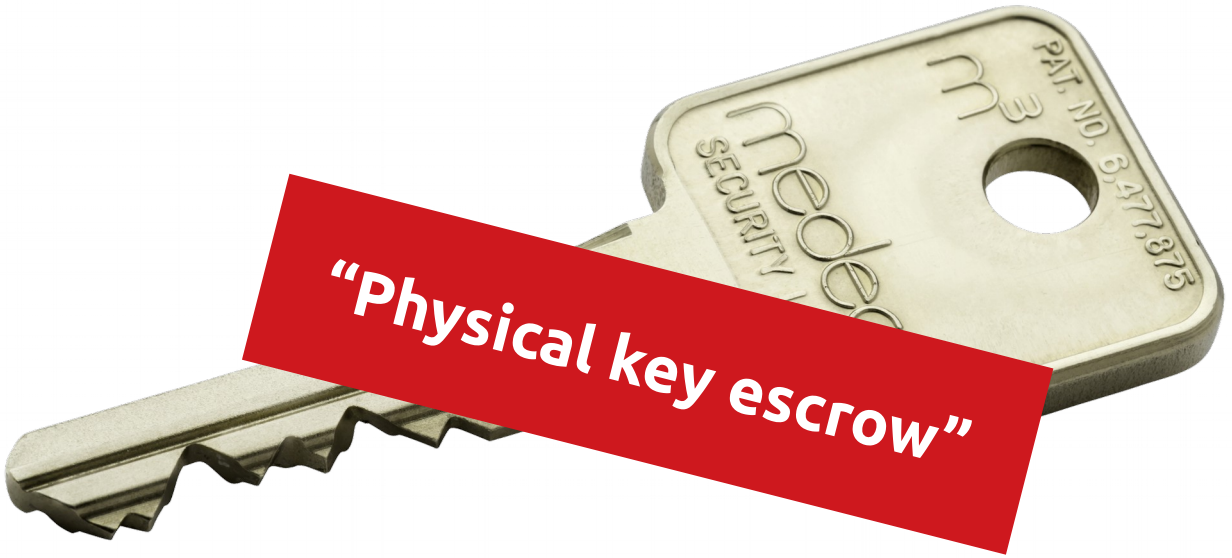

XNH2.5
SERIES 3230


FIRE DEPT
NORMAL OPERATION
EMERGENCY OPEN
KNOX COMPANY PHOENIX, AZ

Knox Boxes



One key





https://www.schneier.com/blog/archives/2011/07/physical_key_es.html


05/29/2016 04:00:48 AM
CH9


05/29/2016 04:00:53 AM
CH9


05/29/2016 04:08:13 AM
CH9


05/29/2016 04:08:19 AM
CH9


05/29/2016 04:08:43 AM
CH10


06/03/2016 03:26:20 AM
CH10



Seattle spending $500,000 to re-key lock boxes after burglaries

POSTED 4:43 PM, OCTOBER 3, 2013, BY STEVE KIGGINS, *UPDATED AT 05:24PM, OCTOBER 3, 2013*



Austin

Security at Austin buildings 'compromised' after burglary suspect gets master key

By: Calily Bien

Posted: Jan 09, 2018 10:10 AM CST
Updated: Jan 09, 2018 10:10 AM CST

[citation needed]



[citation needed]



[citation needed]




05/29/2016 04:08:13 AM
CH9



FOX 7 ☰ Sections News Weather Good Day FOX 7 Features Contests Traffic

Local Texas US & World Politics Business Health Entertainment Strange Trending

'Knox Box' master key theft compromises thousands of buildings across Austin

Phoenix Fire Department Loses 850 Keys, Which Access Thousands of Local Businesses and Apartments



Phoenix Fire Department Loses 850 Keys, Which Access Thousands of Local Businesses and Apartments



The locks


KNOX
medeco
MDL 3200 SERIES
SN 32-535-032
OUTDOOR USE
THE KNOX COMPANY, PHOENIX, AZ

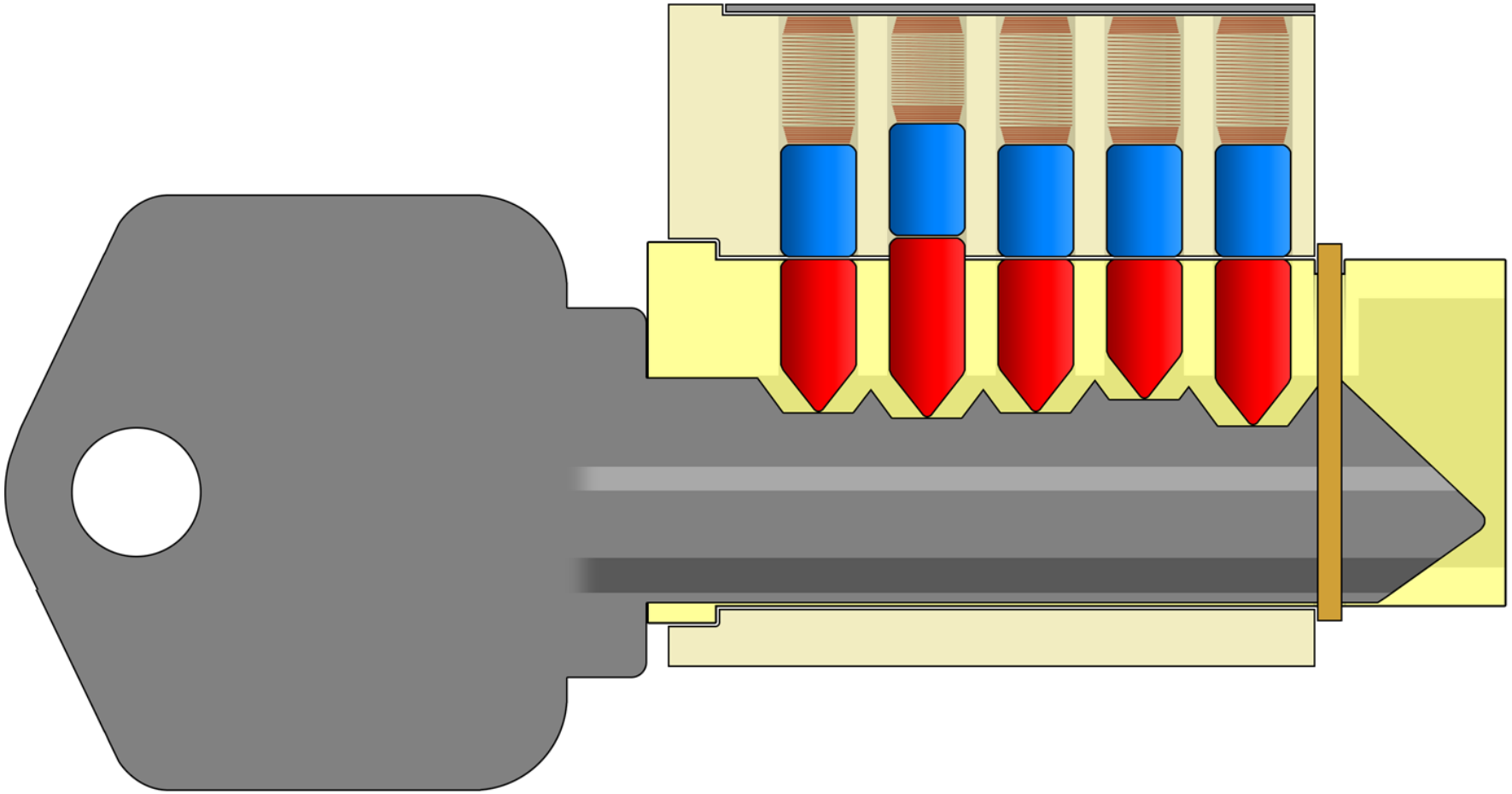
The locks

medeco®
HIGH SECURITY LOCKS

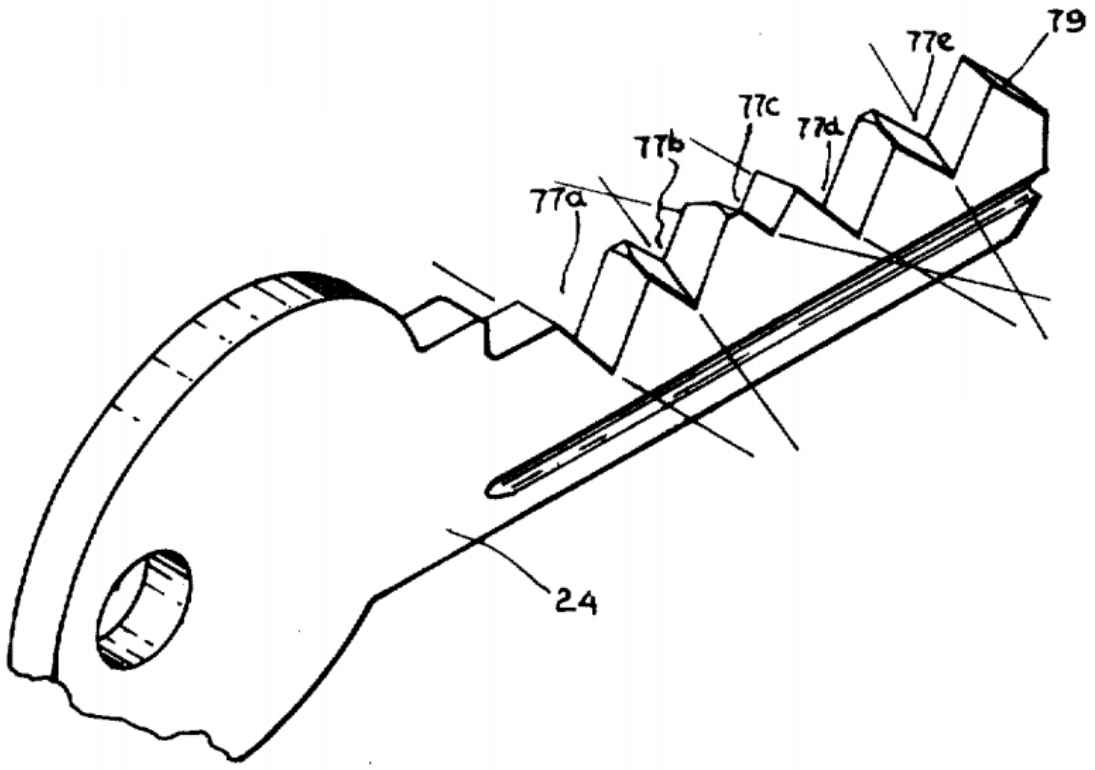
ASSA ABLOY



The locks



The locks



The locks



The locks



The locks

UL LISTED



UL 1037



UL 437

The locks







UL 1037

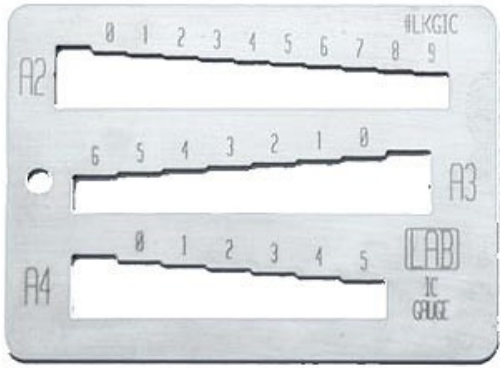
UL 437

Key control



Knox KeySecure

Key control



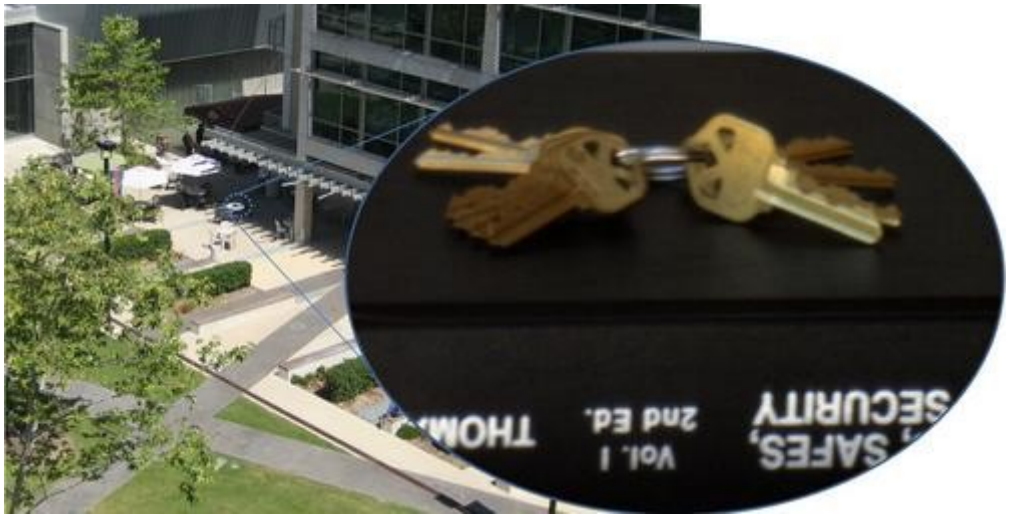




Key control

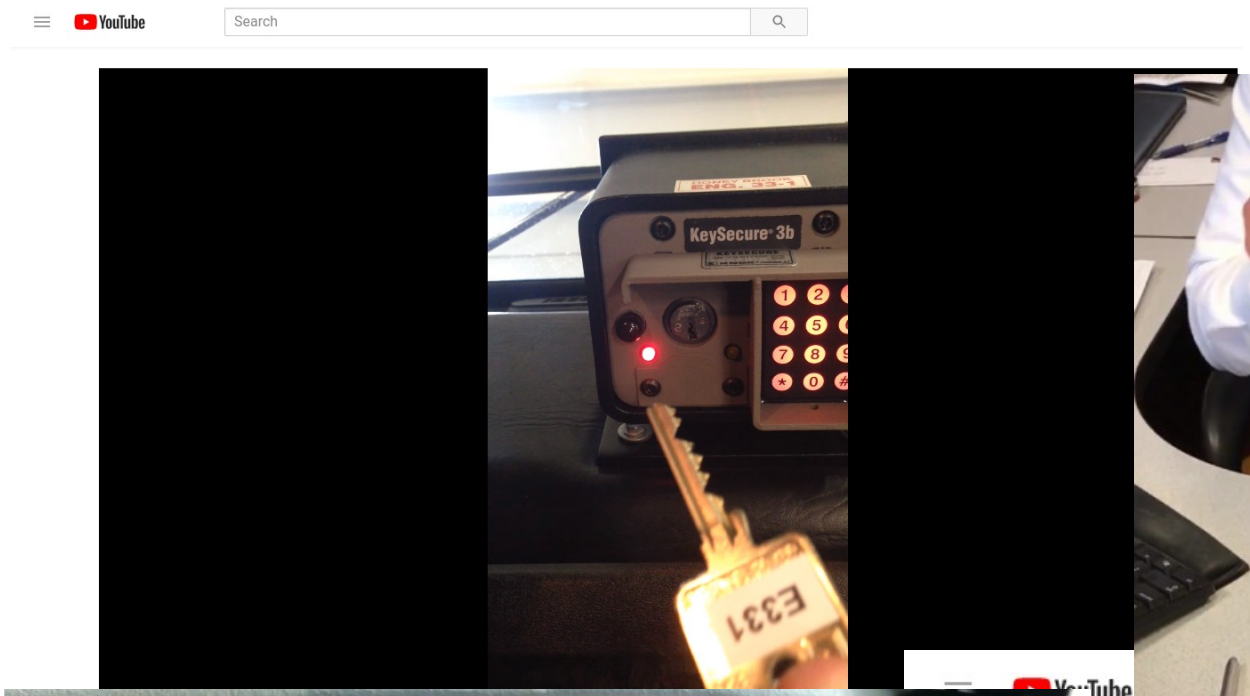


Key control



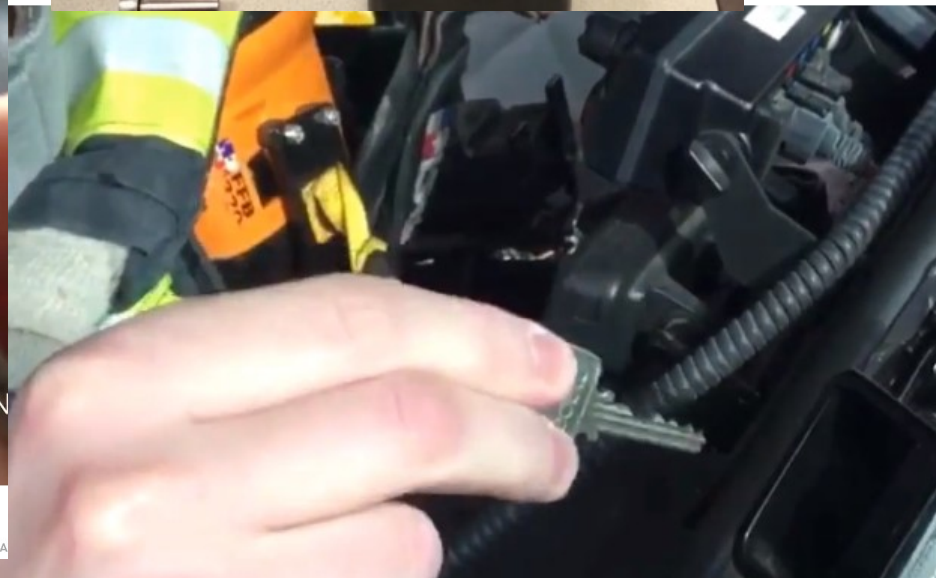


“Key control”









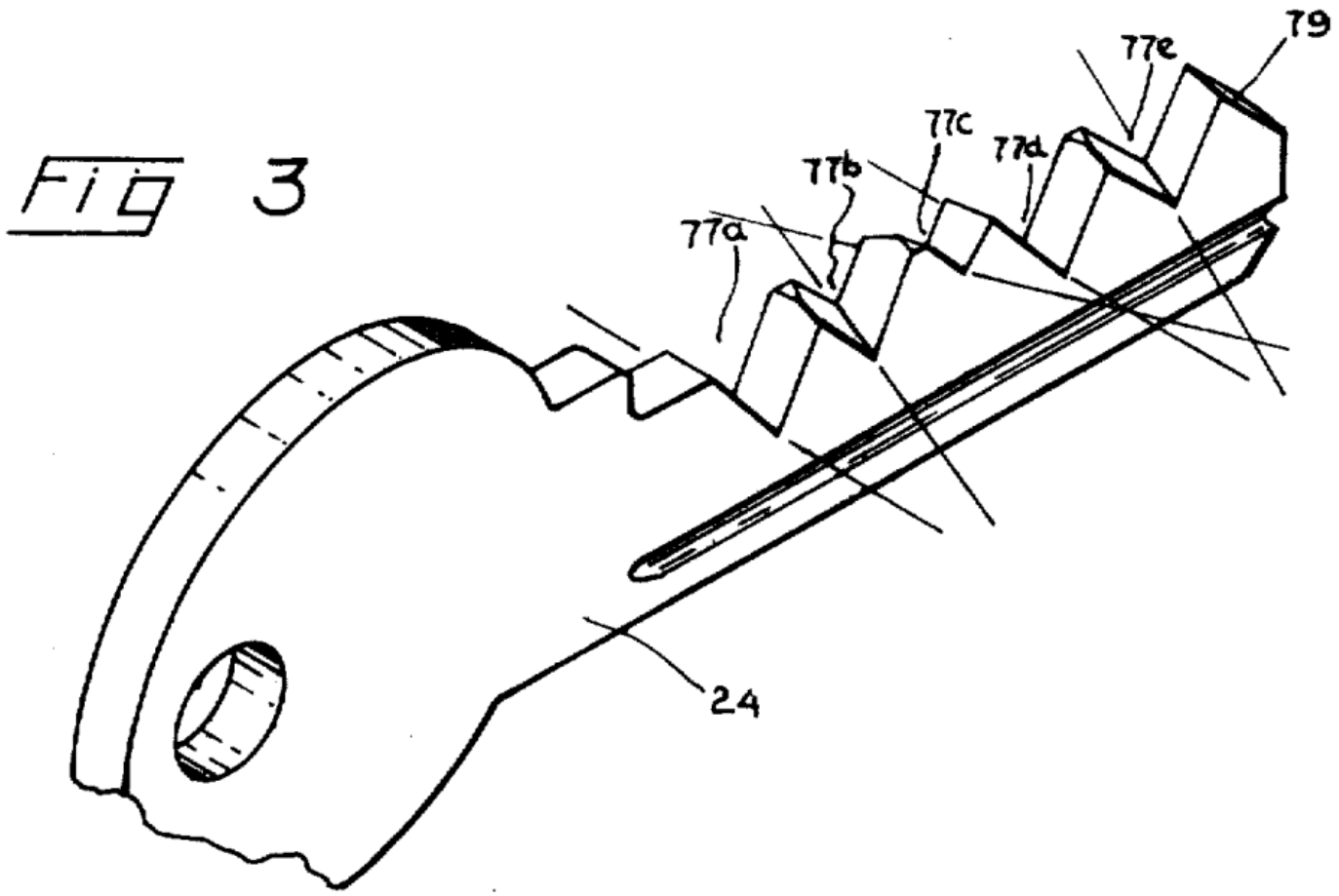
Belltown FD---Knox Box Release Training Video

784 views

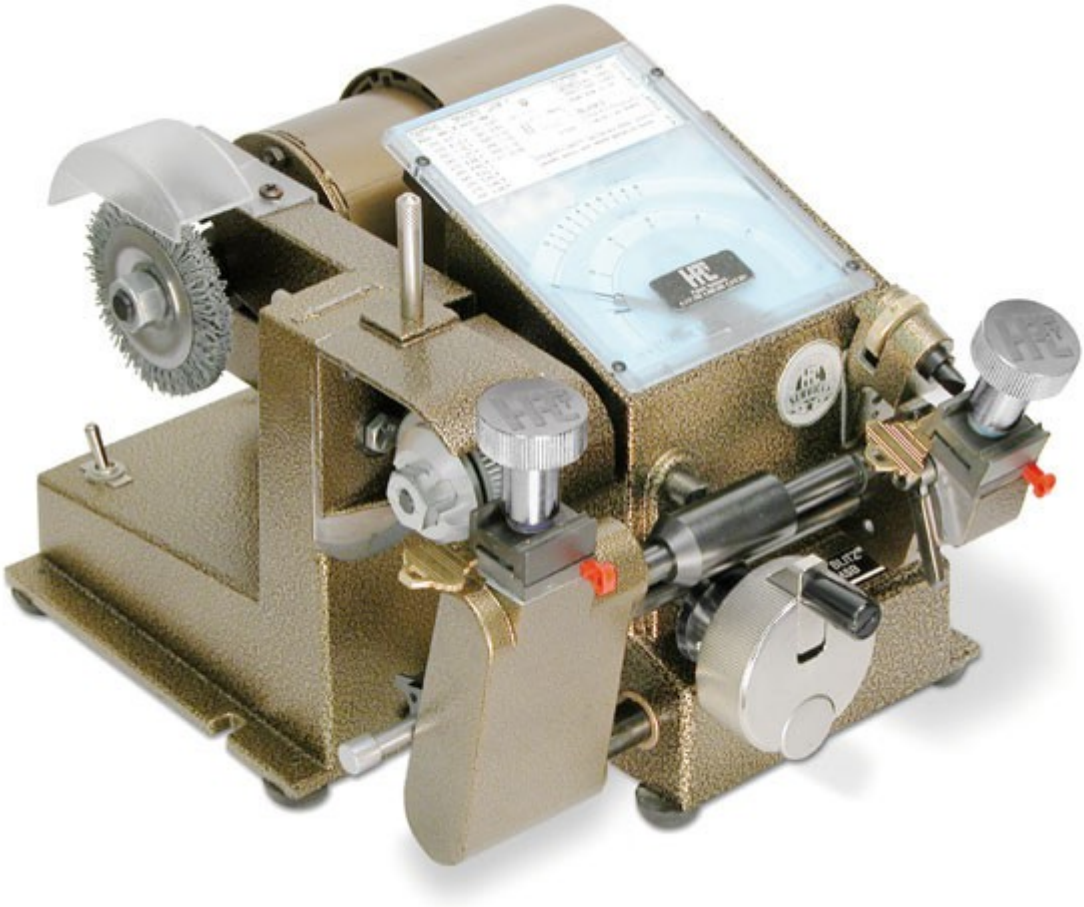
Key control



Key control?



Cutting keys

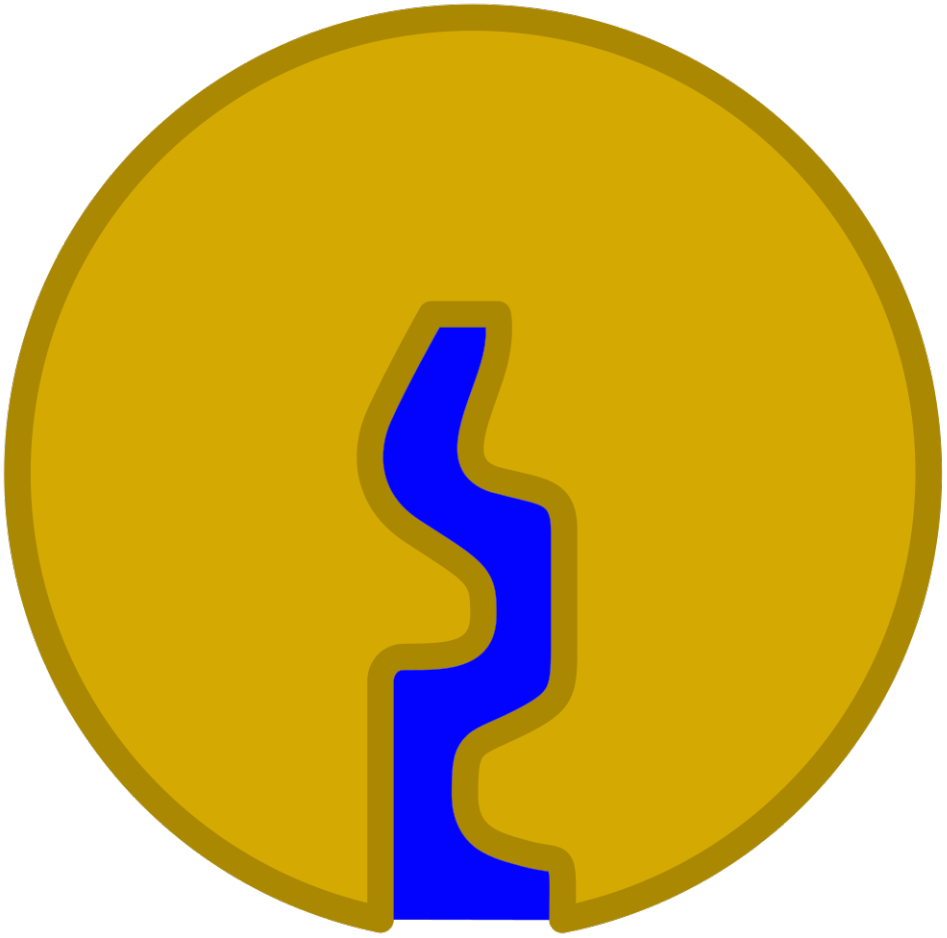


HPC Blitz

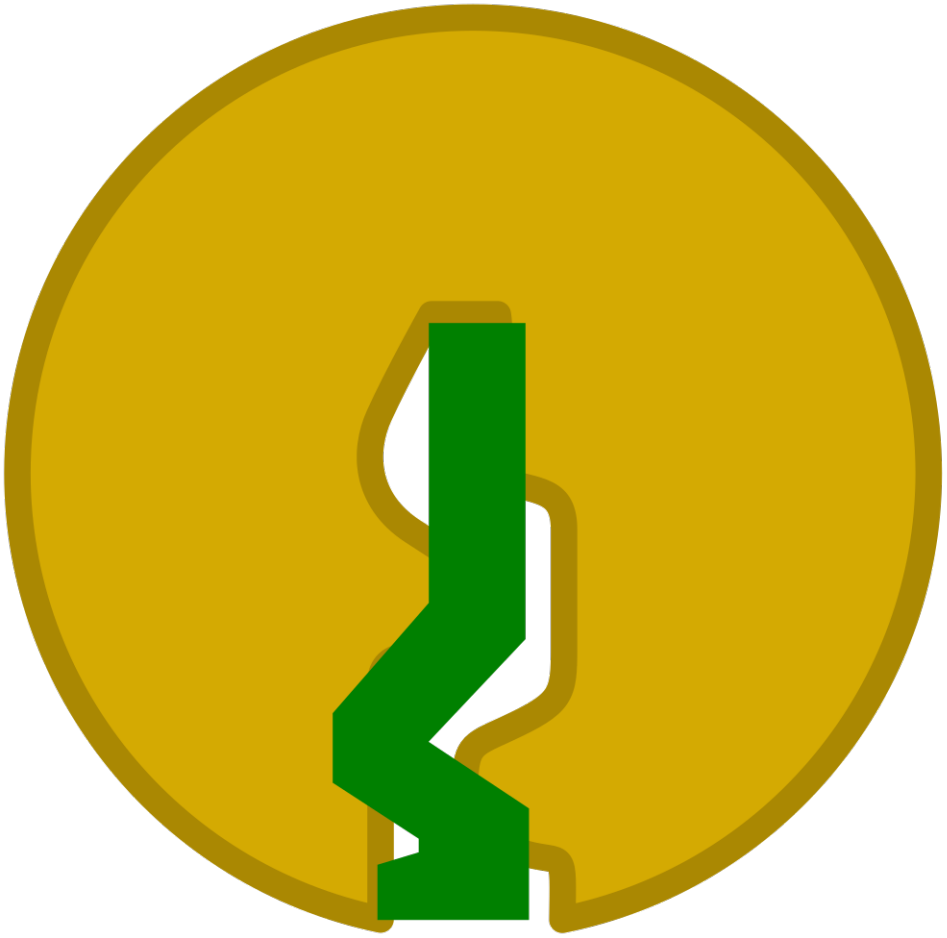
Blanks



Making blanks



Making blanks



Making blanks



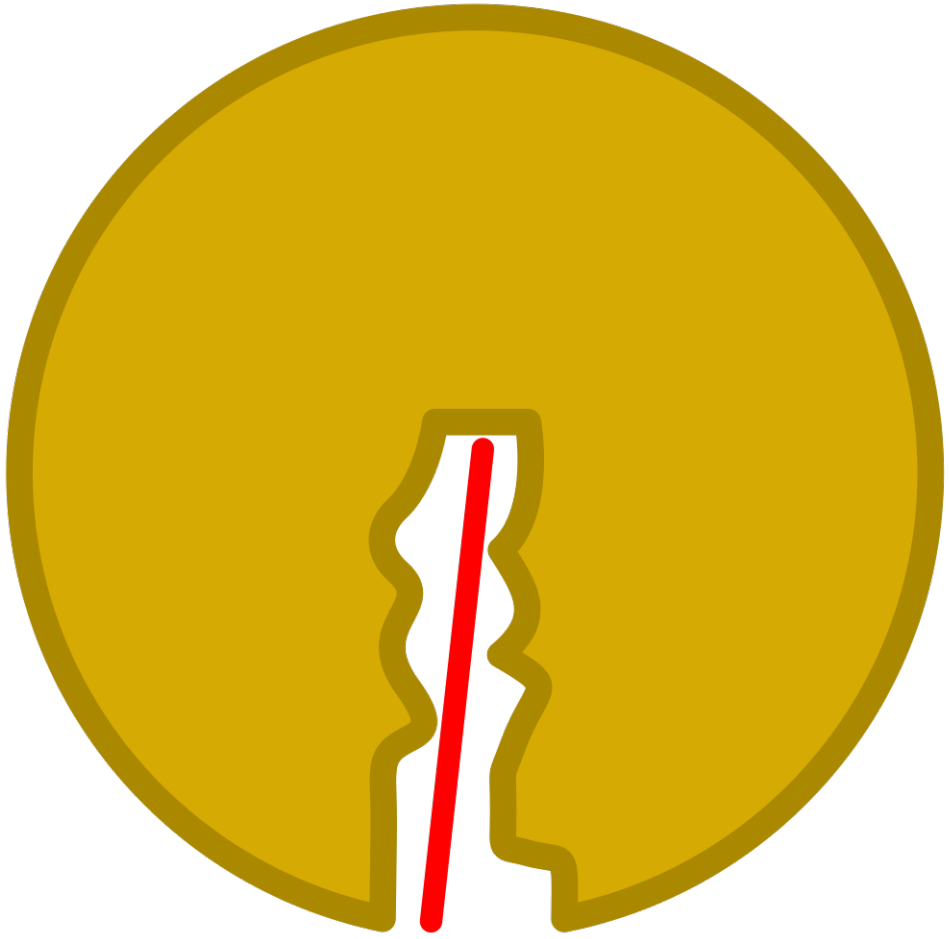
Making blanks

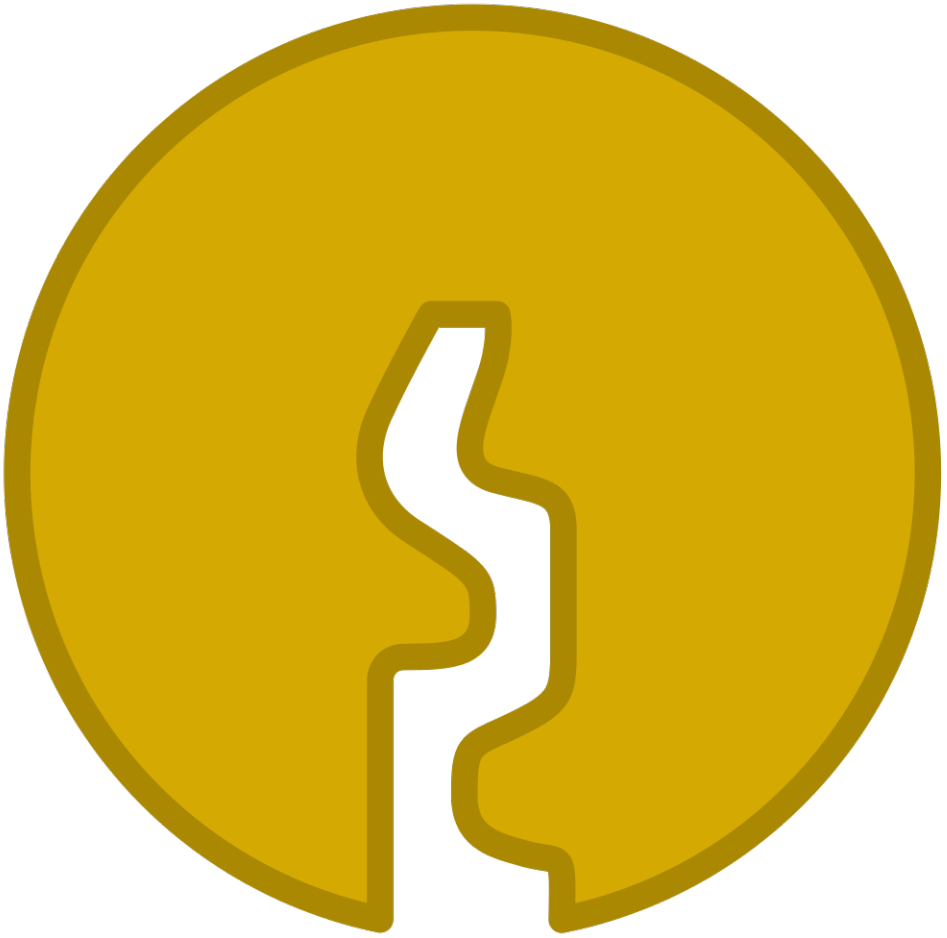


Making blanks



Making blanks

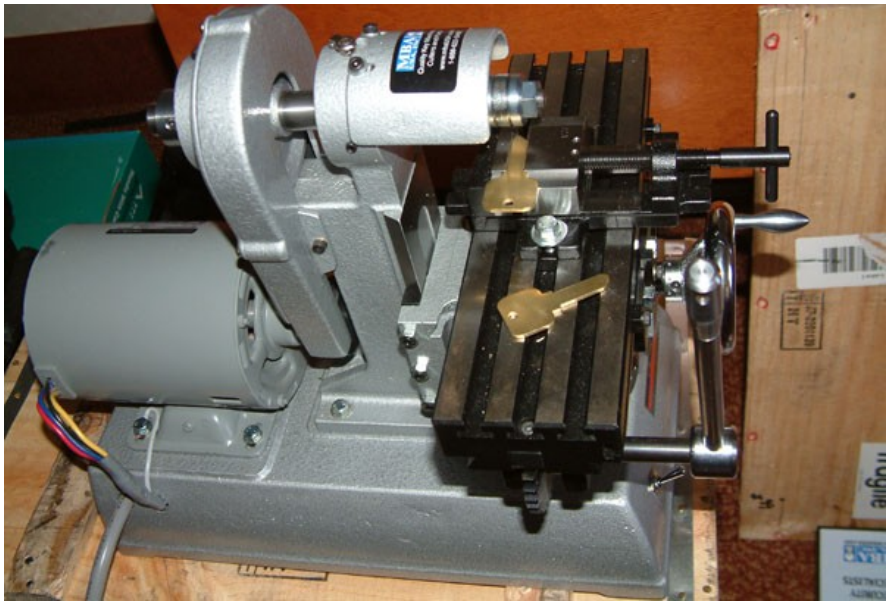




Making blanks



Making blanks



Keyway King



Easy Entrie

3d printing





3d printing





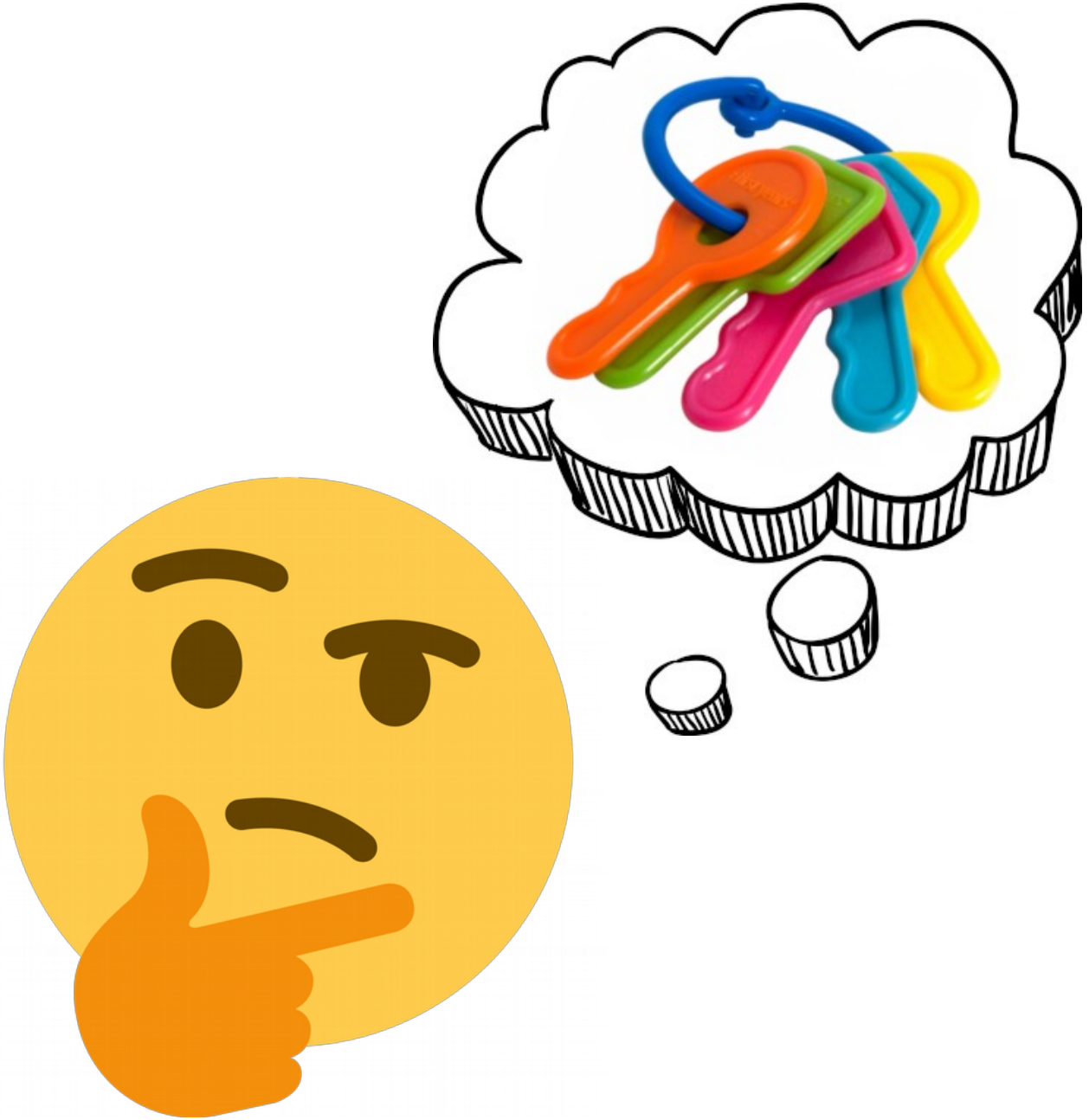
3d printing

shapeways

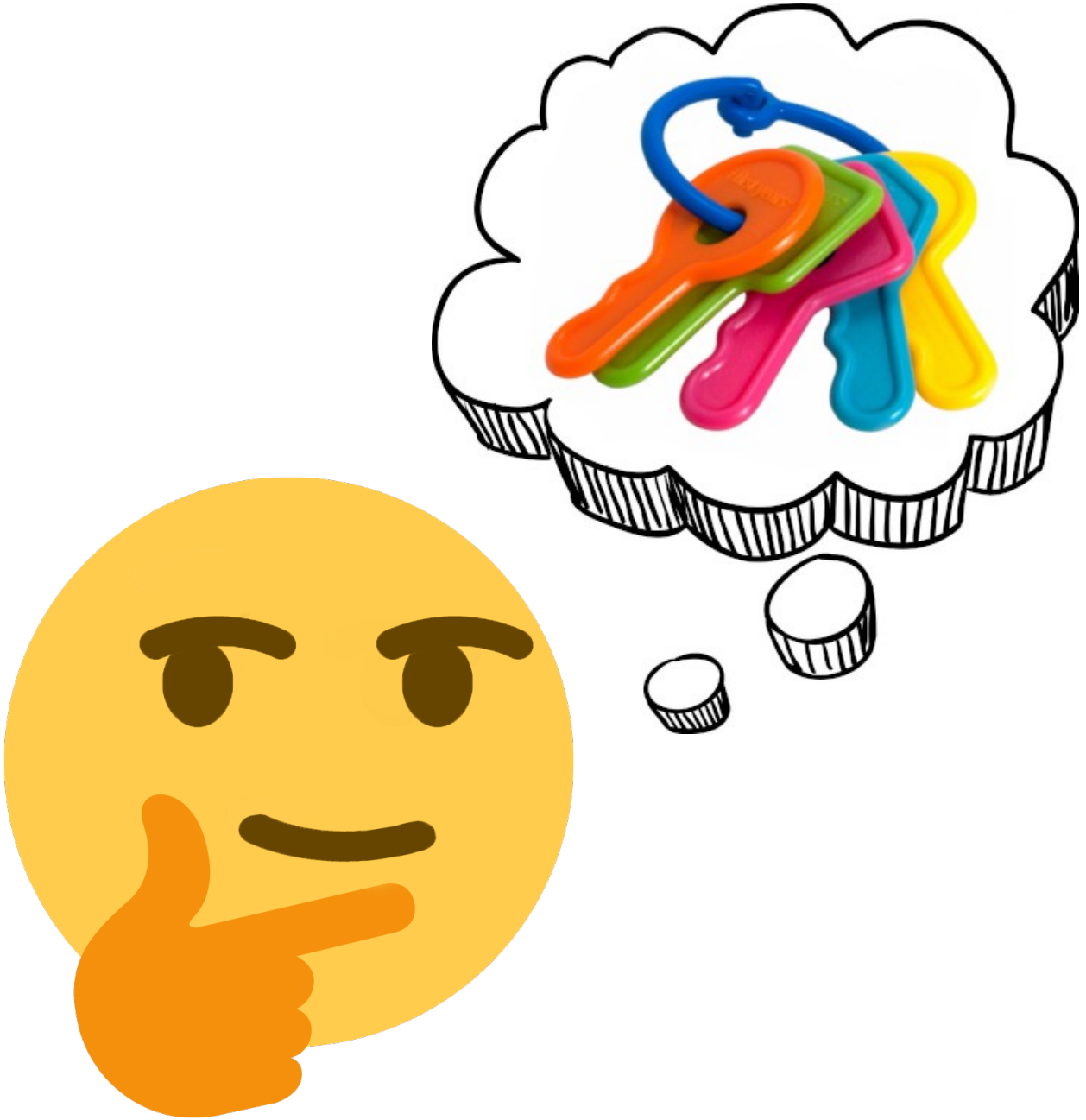




Hmmm



Hmmm



Key control



US006945082B2

(10) **Patent No.: US 6,945,082 B2**

(45) **Date of Patent: Sep. 20, 2005**

Key control





Key control



Key control?





Investigating the box



Investigating the box



Investigating the box



Investigating the box



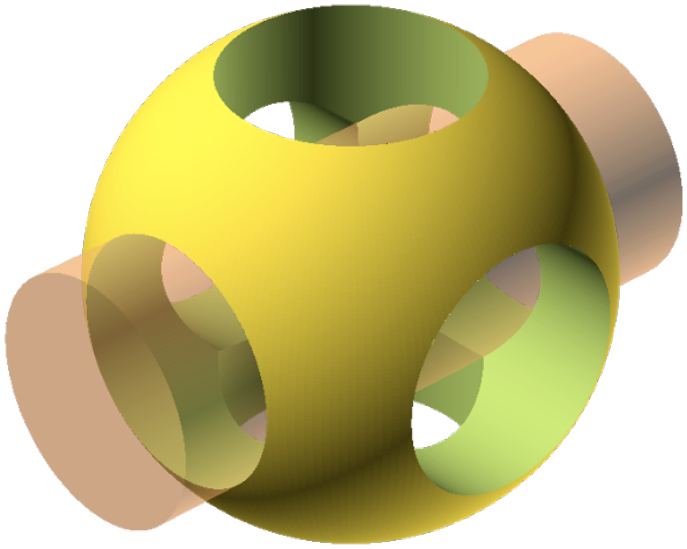
Investigating the box



Investigating the box



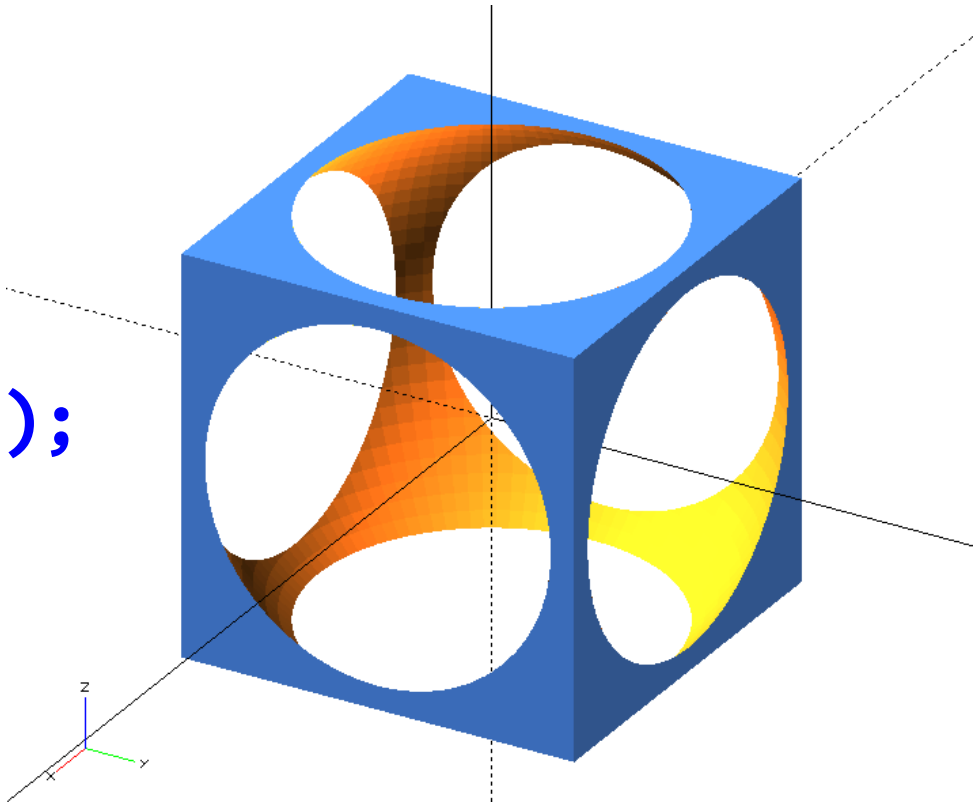
OpenSCAD



OpenScad

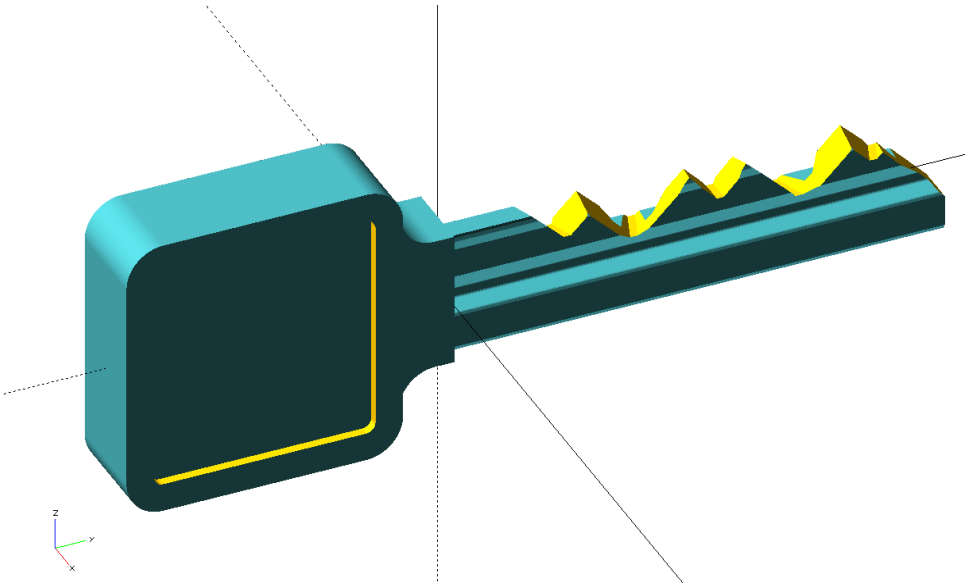
OpenSCAD

```
$fn = 100;
difference() {
      cube(3, center=true);
      sphere(2);
}
```

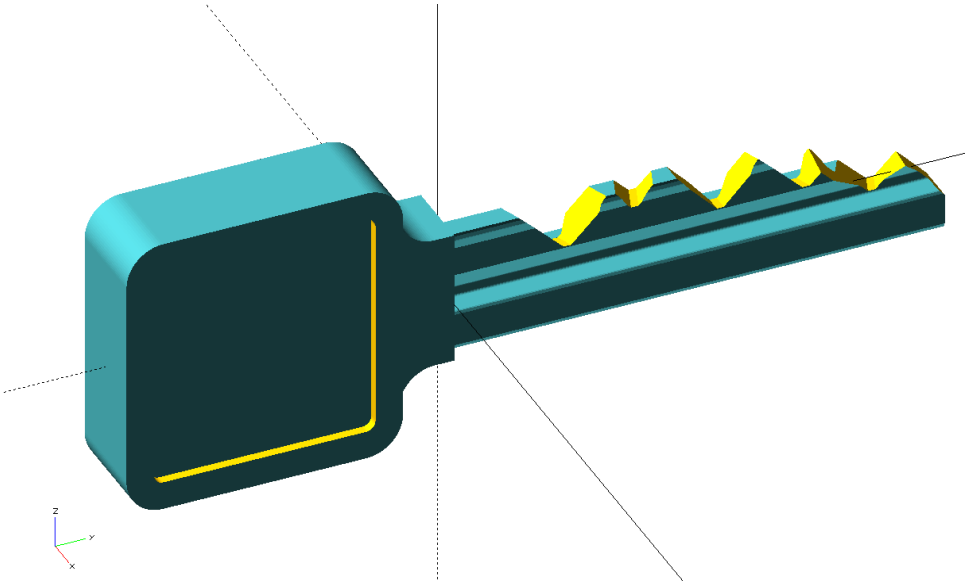


OpenSCAD

```
depths(2,4,2,4,2);
```



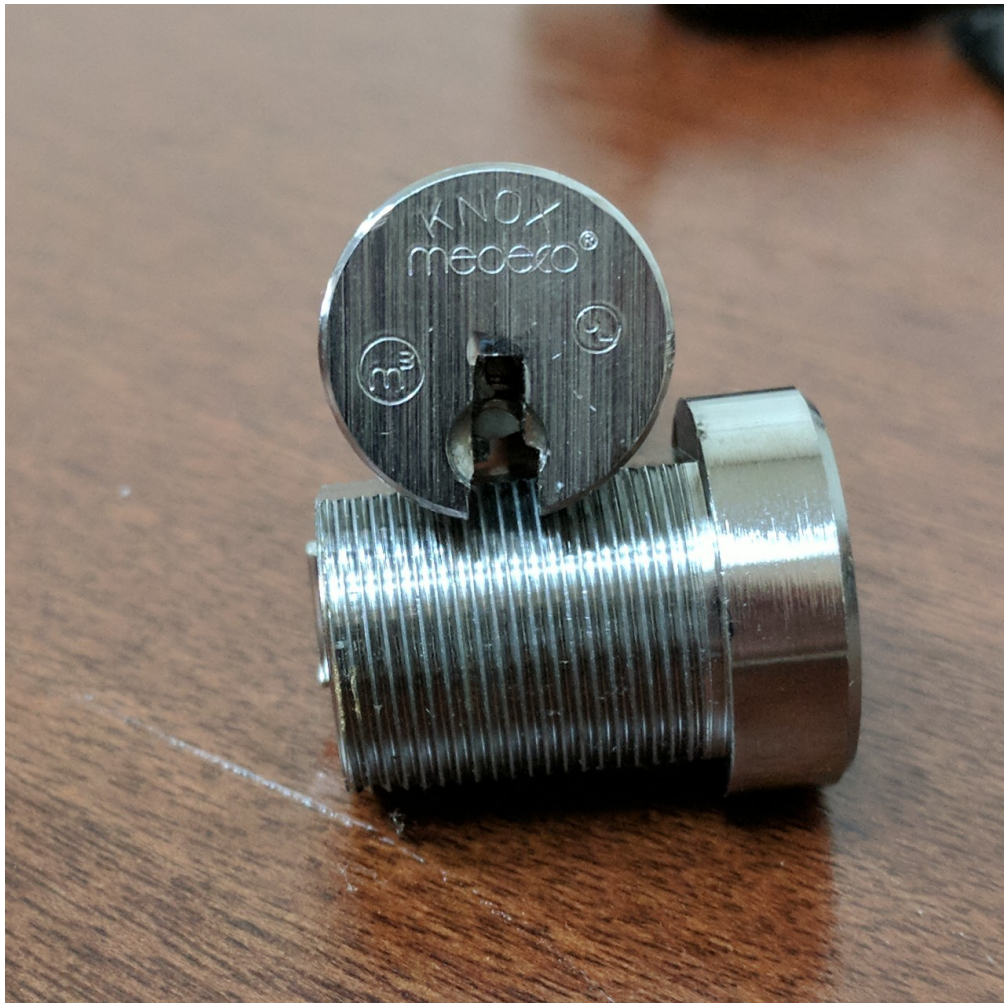
```
depths(3,1,3,3,7);
```



Prior art

- Nirav Patel
  - eclecti.cc
- Christian Holler
  - autokey3d
- Eric Van Albert
  - keygen.co

Modeling the keyway



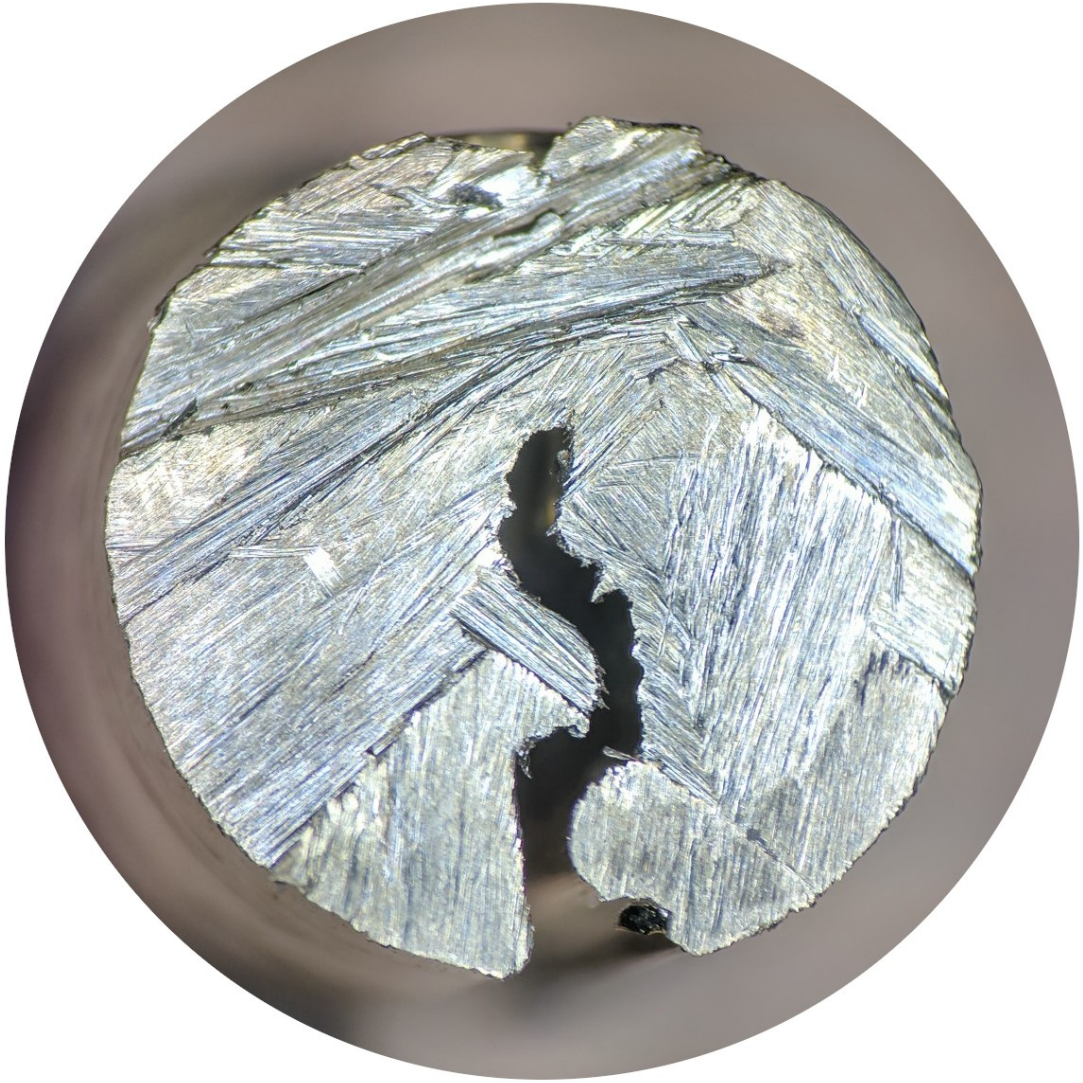
Modeling the keyway



Modeling the keyway



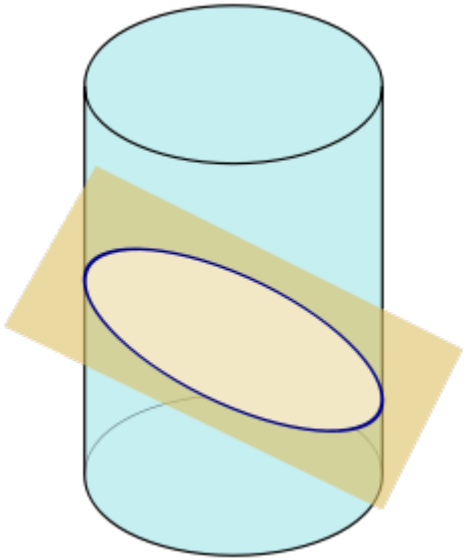
Modeling the keyway



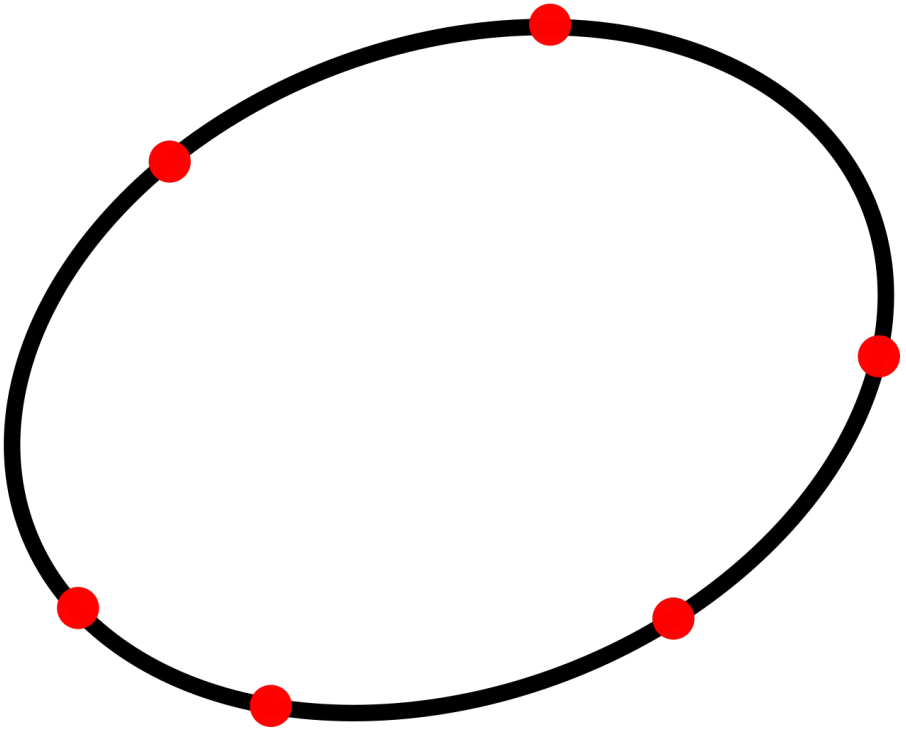
Modeling the keyway



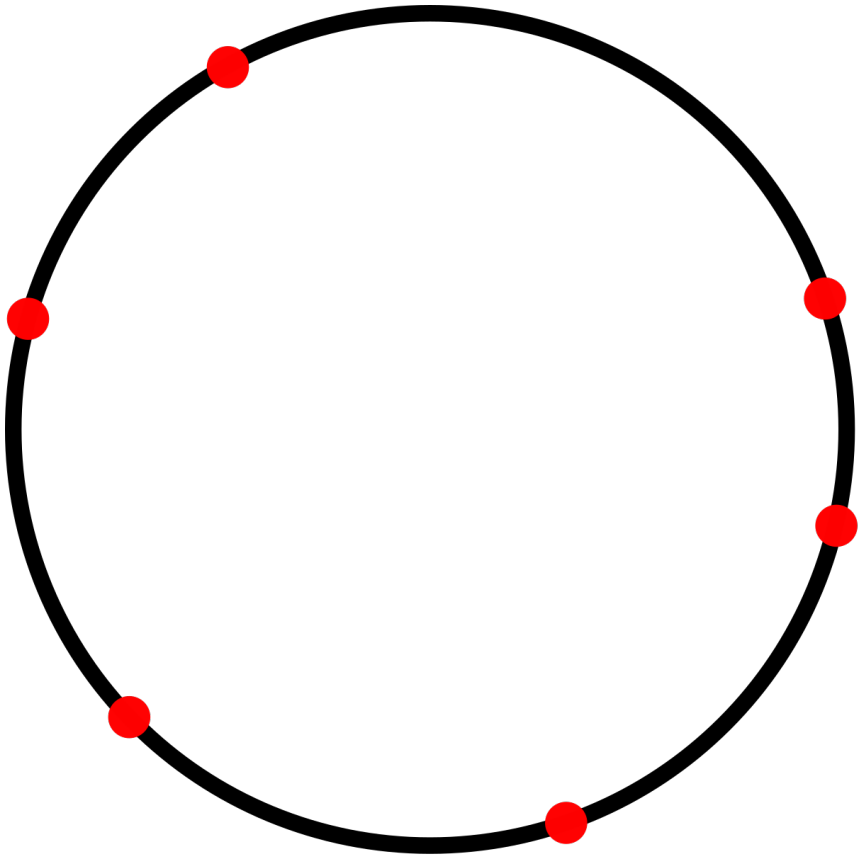
Modeling the keyway



Modeling the keyway



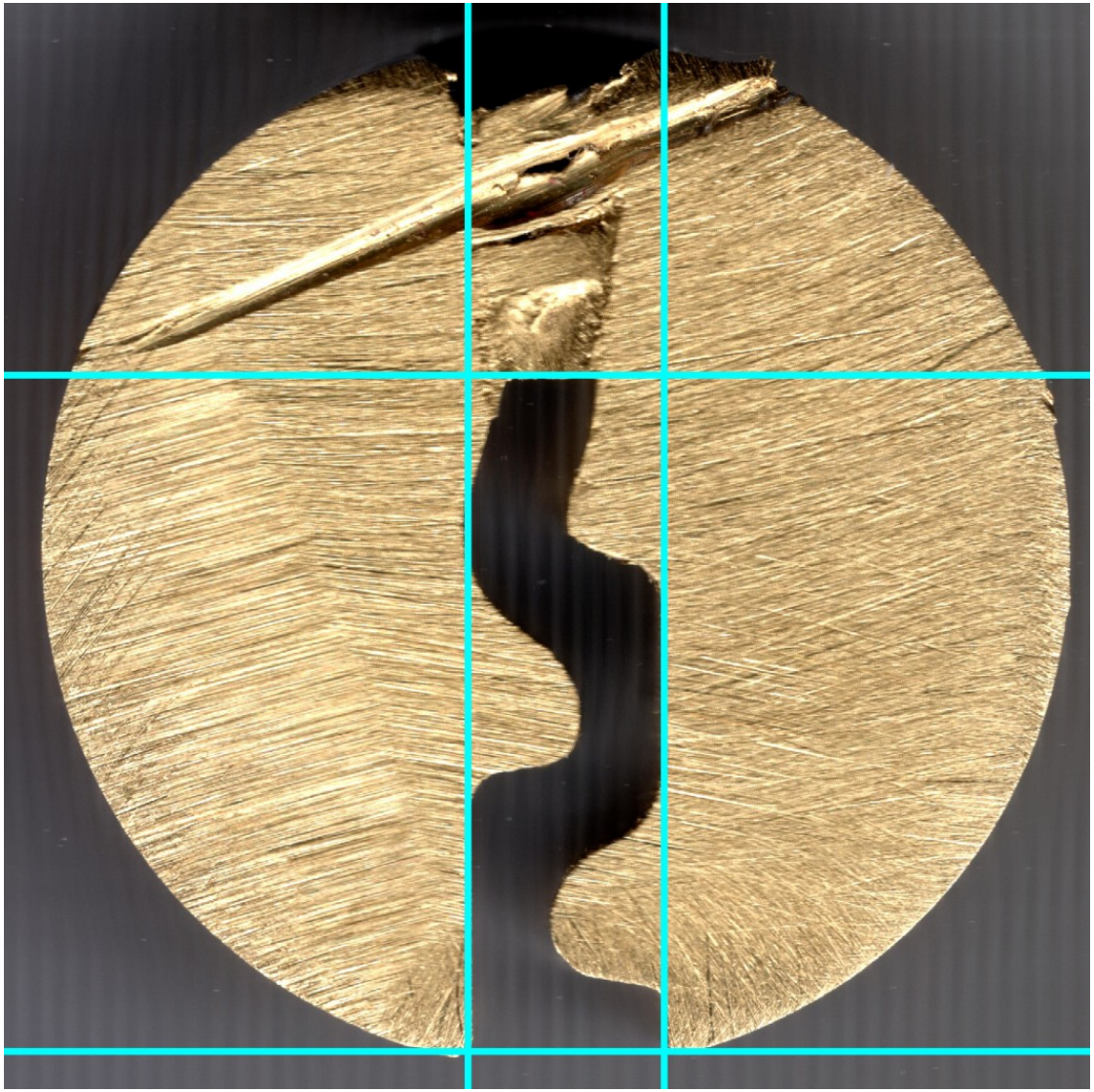
Modeling the keyway



Modeling the keyway



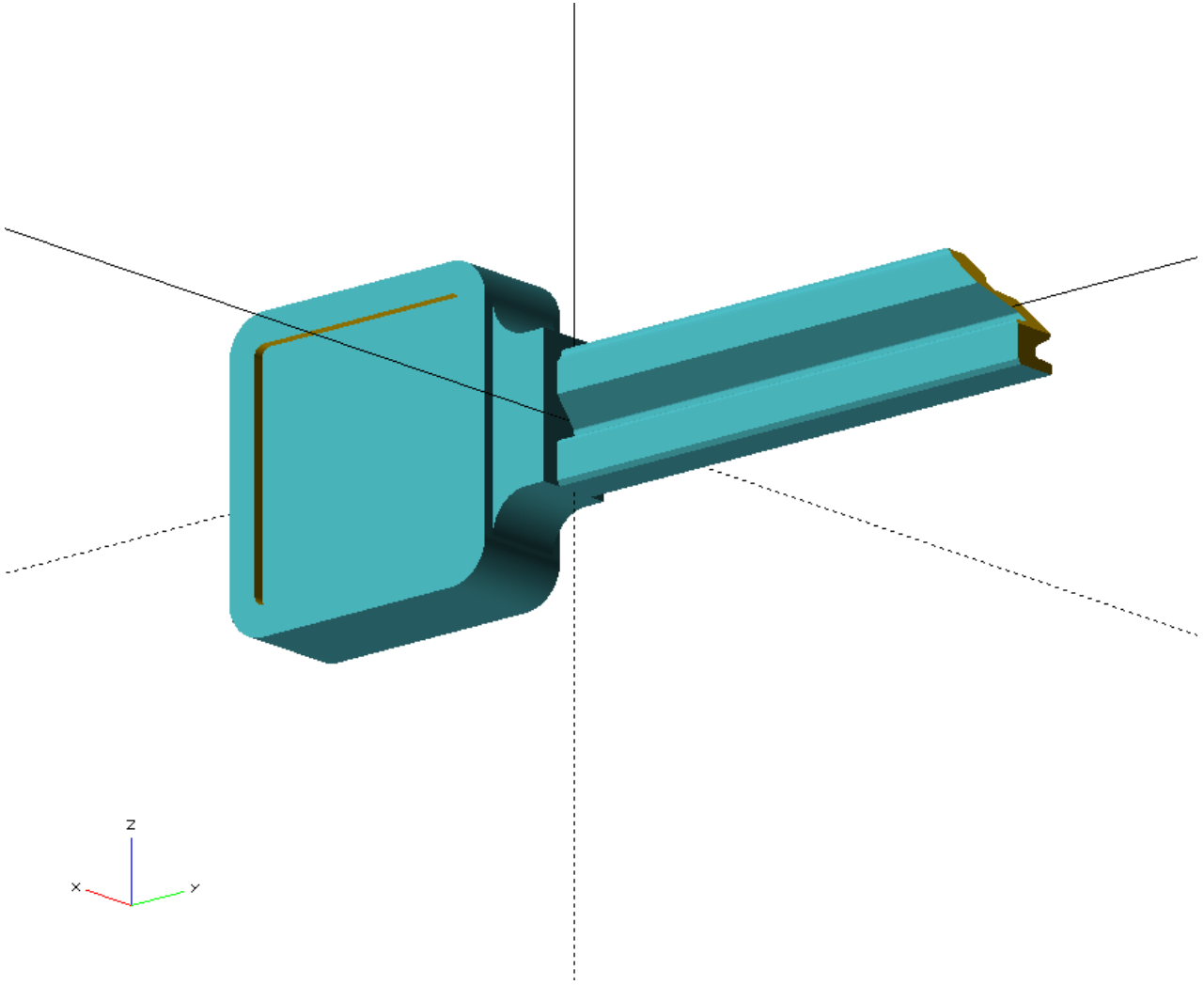
Modeling the keyway



Modeling the keyway



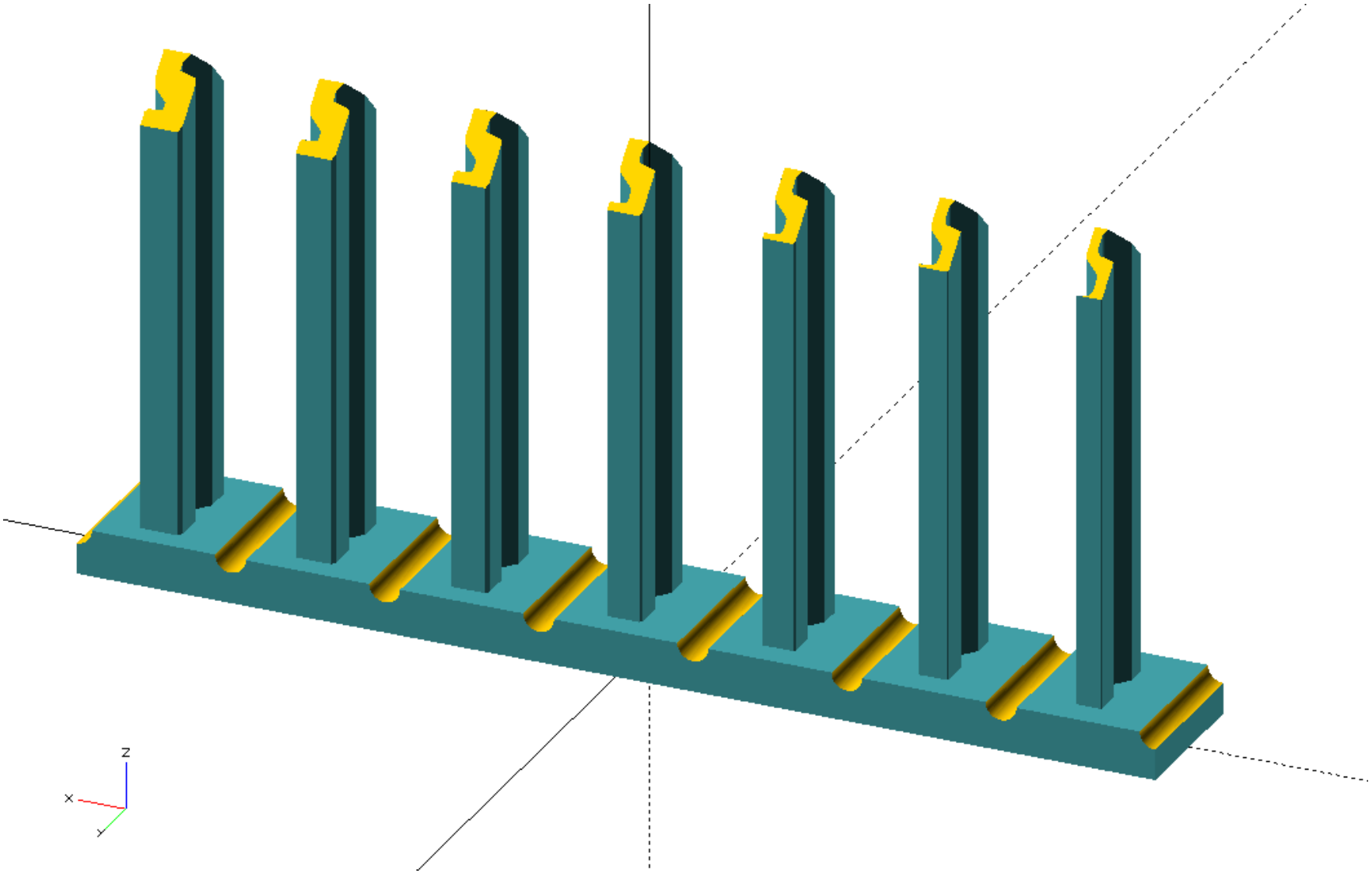
Modeling the keyway



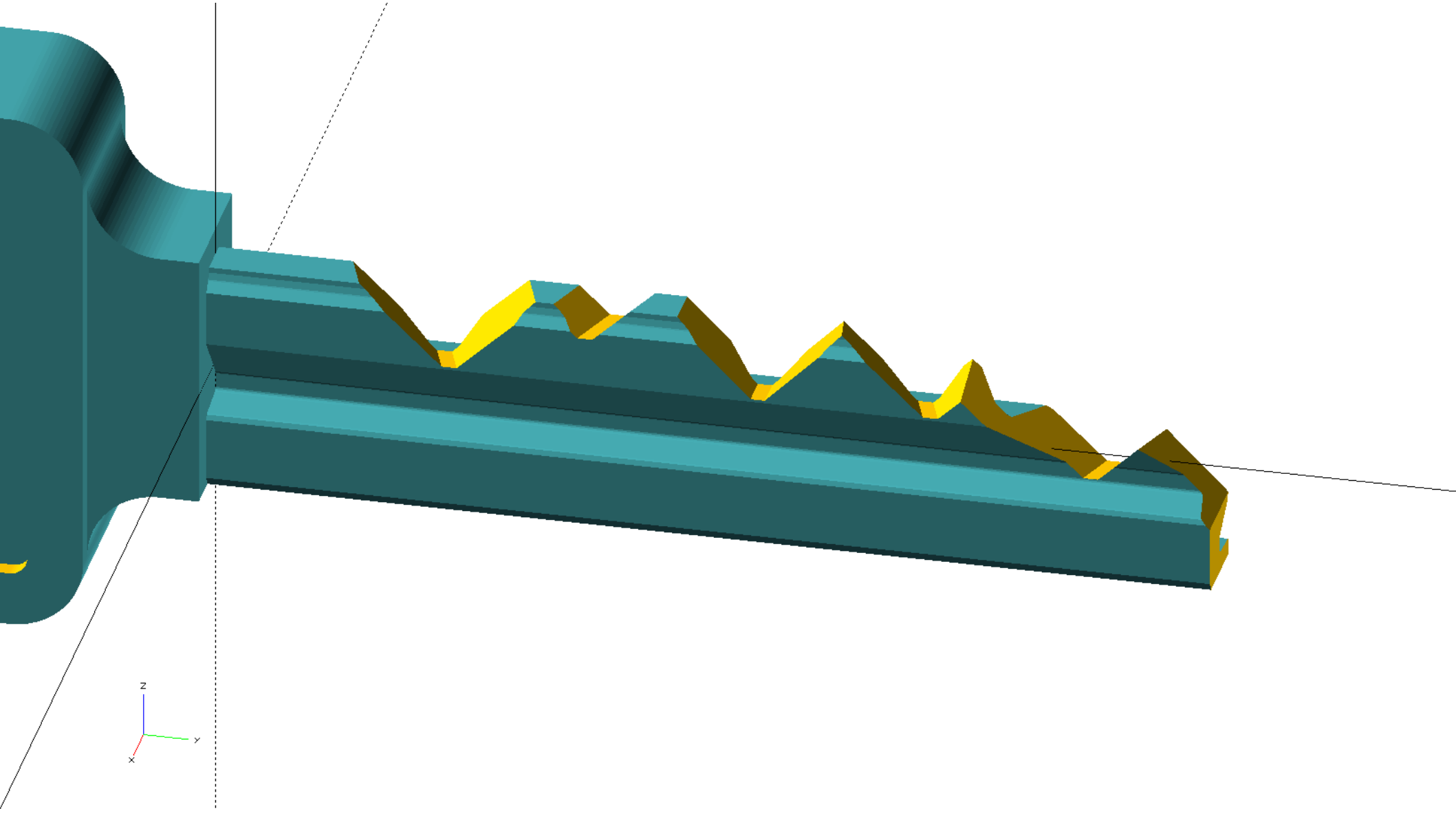
Modeling the keyway



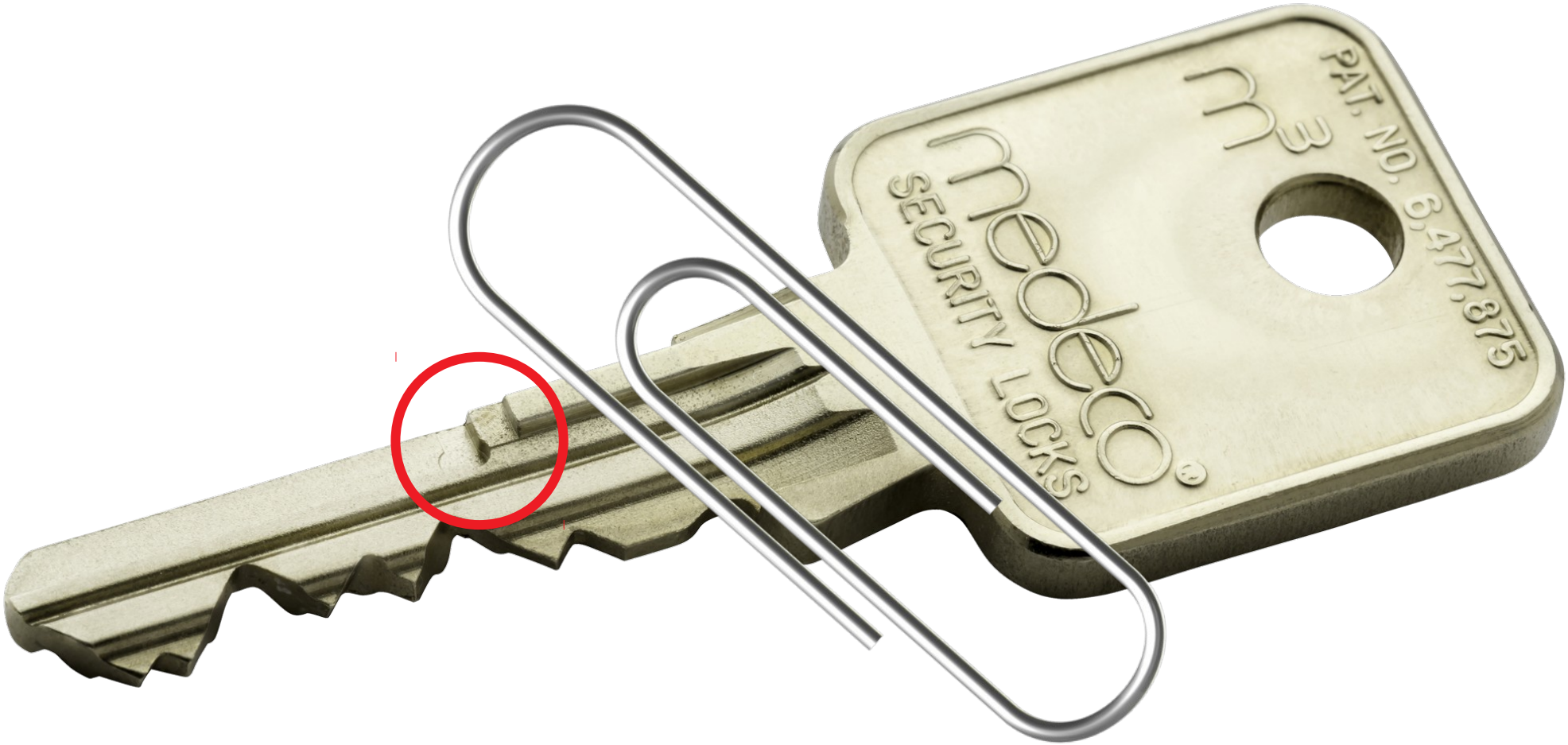
Modeling the keyway

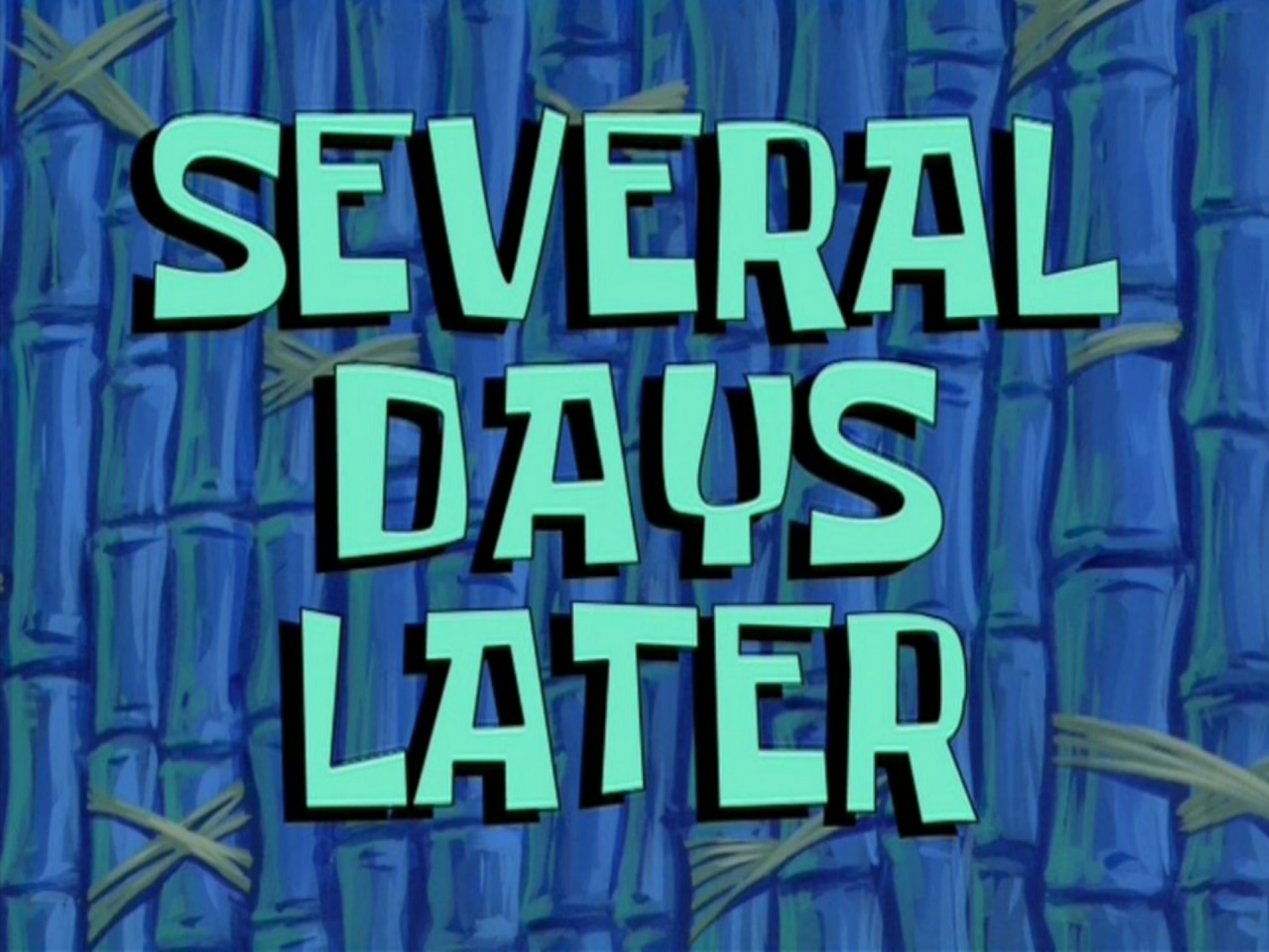


Modeling the cuts



M3 element




SEVERAL
DAYS
LATER

Pwned



Pwned



Sturdy



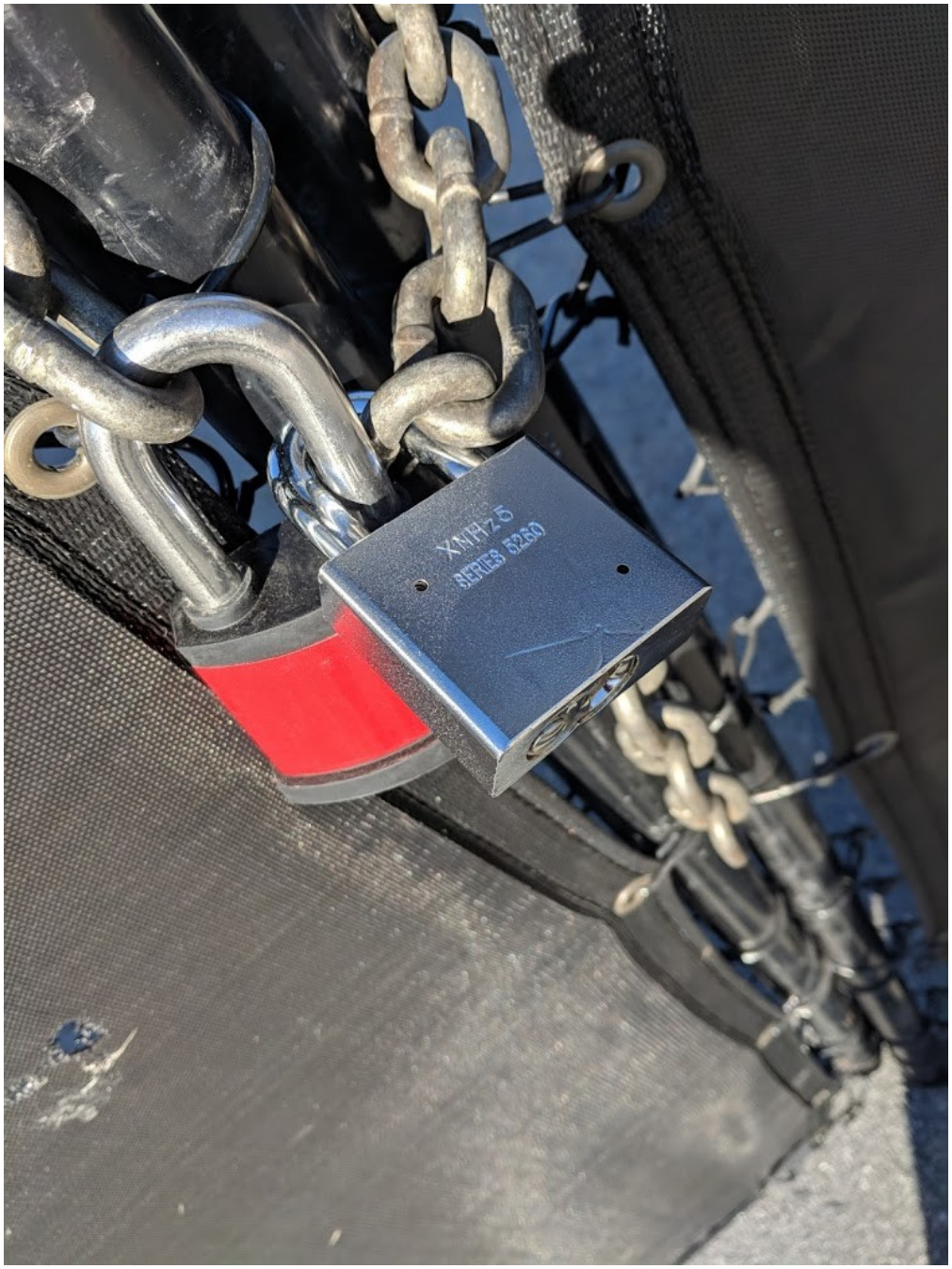
Very difficult to steal





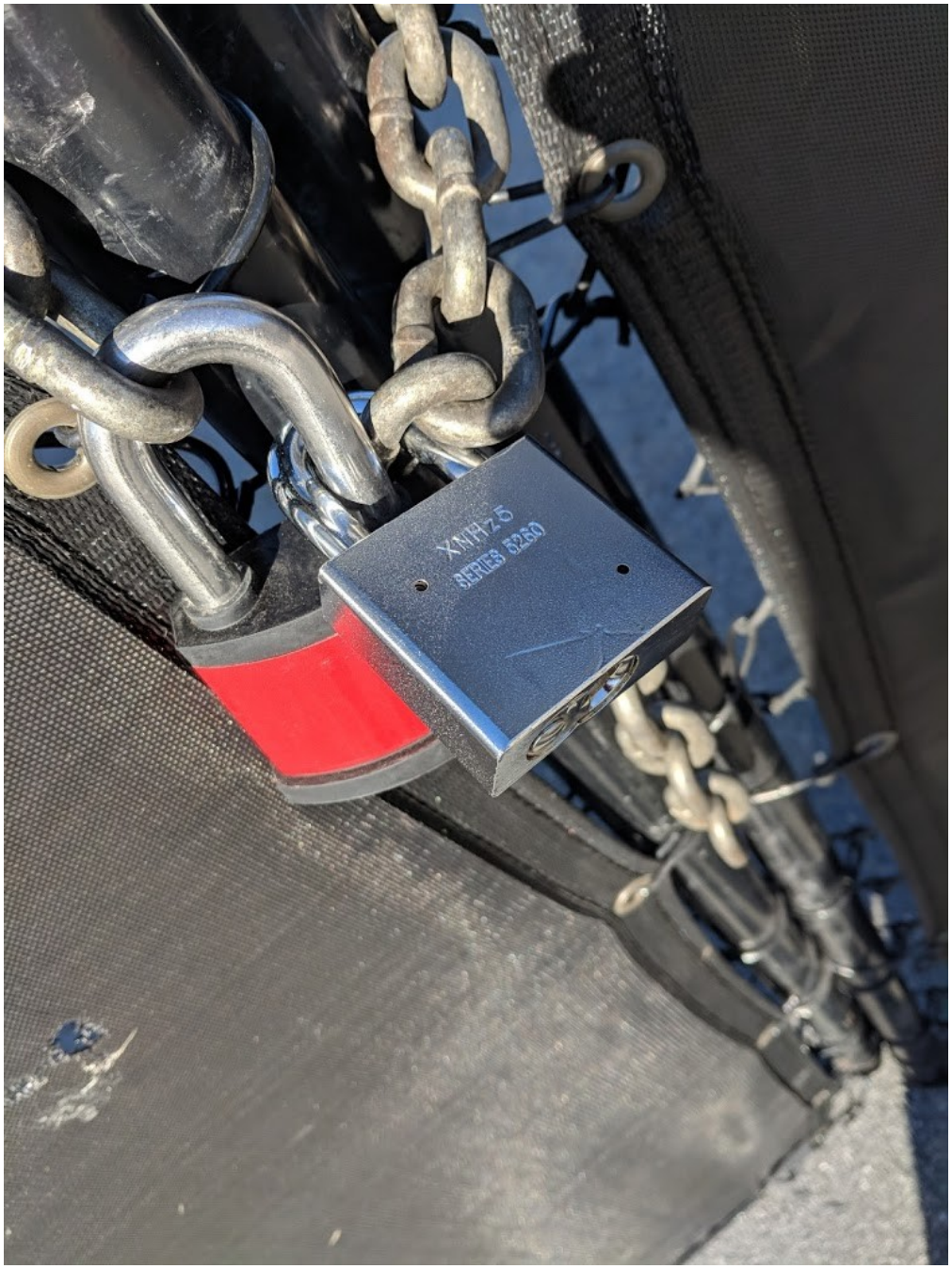
Very difficult to steal





Very difficult to steal



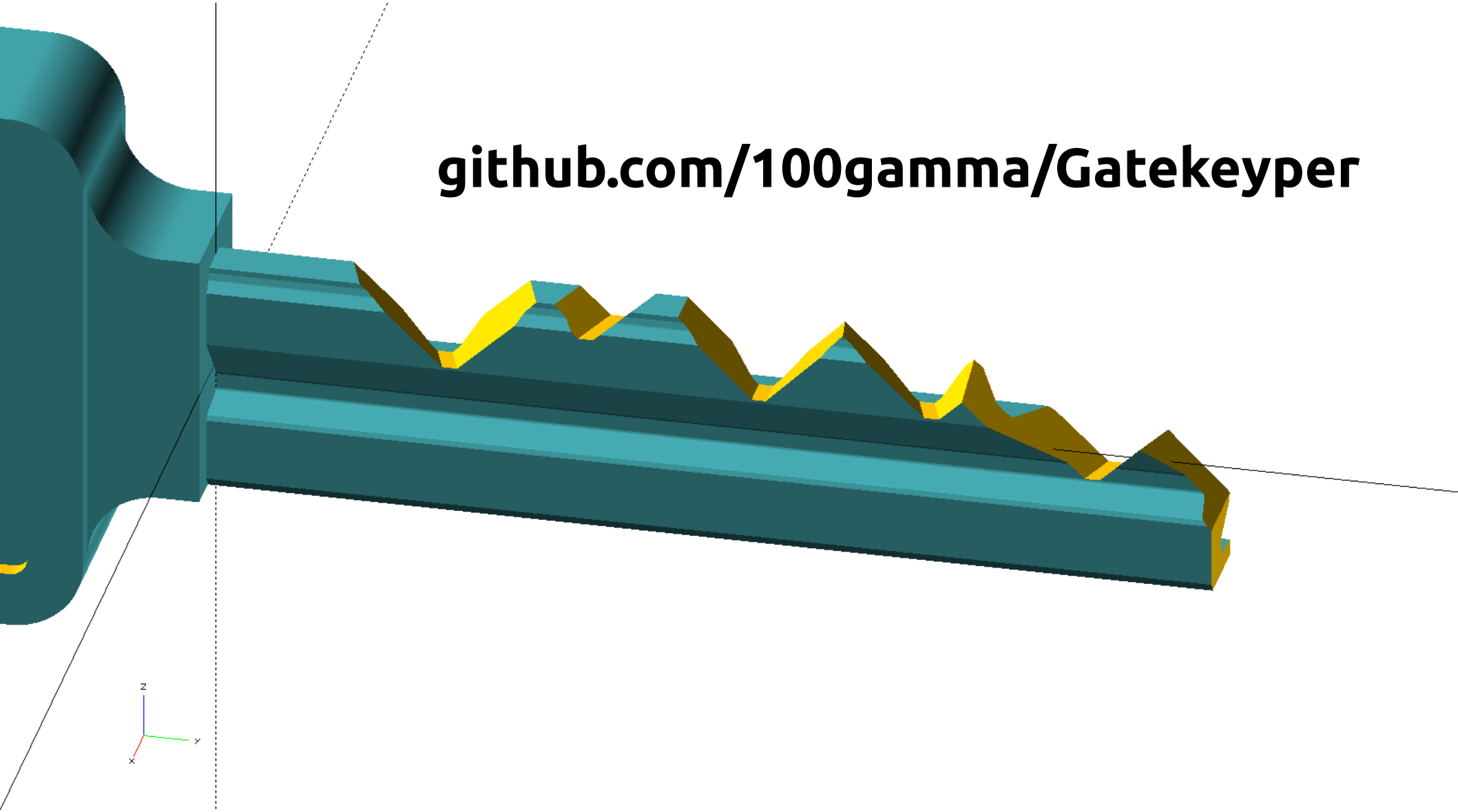


Very difficult to steal





Gatekeyper



Change the locks?





Electromechanical locks



Electromechanical locks



Electromechanical locks





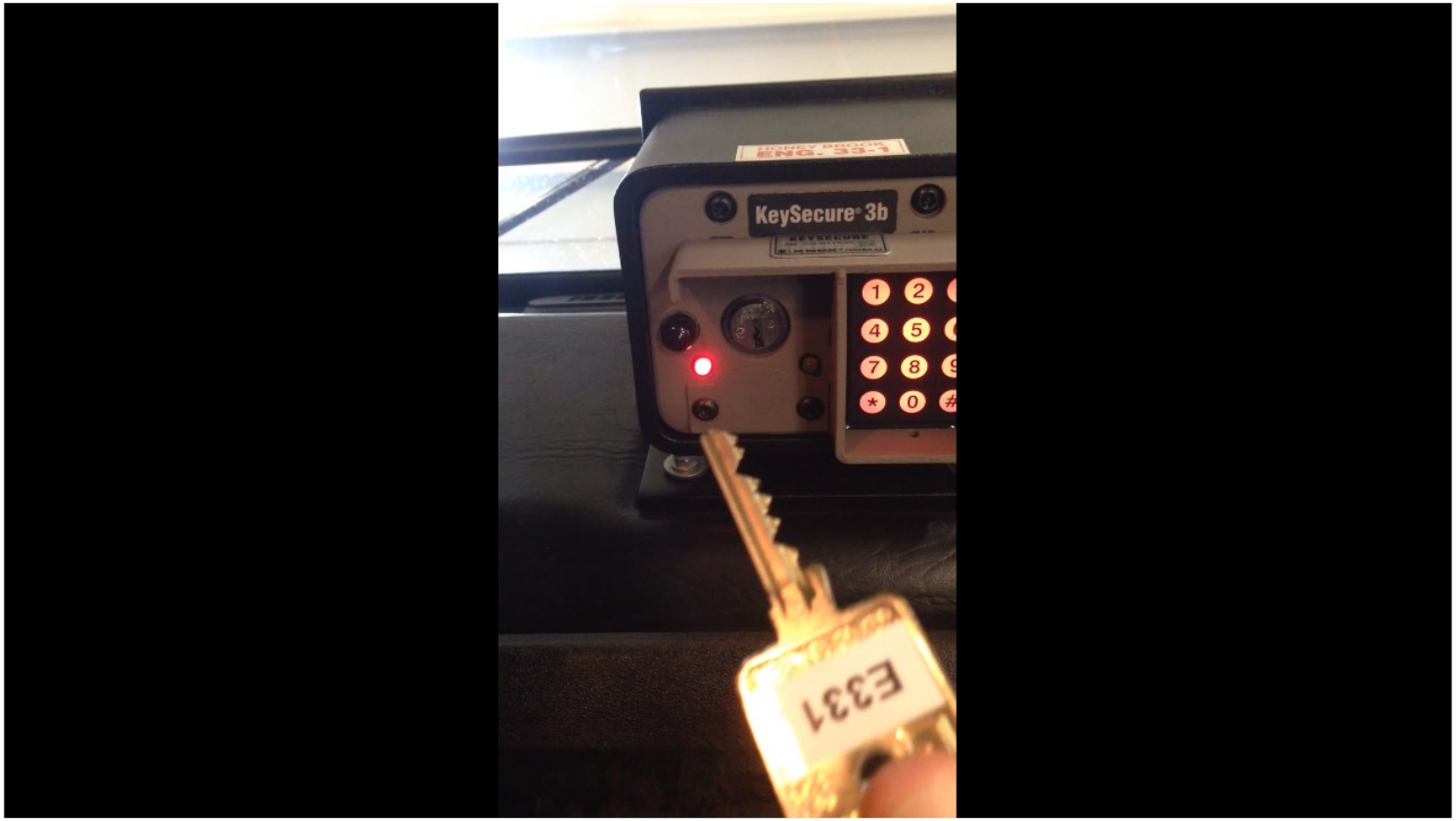
Combination locks



Stanton Concepts Robo Key System

YouTube

Search



Knox Box Tutorial

4,386 views

11 1 SHARE

Robert Klinger Jr.
Published on Mar 18, 2015

SUBSCRIBE 350

Category	Nonprofits & Activism
License	Standard YouTube License

Knox eLock


KNOX
1
2
3
MDL 3200 SERIES
SN 32-468028
OUTDOOR USE
THE KNOX COMPANY, PHOENIX, AZ

[CITATION NEEDED]



http://www.videos.fireengineering.com/detail/videos/fdic-2018/video/5786166707001/

[CITATION NEEDED]



https://www.youtube.com/watch?v=TC34dDzSdus

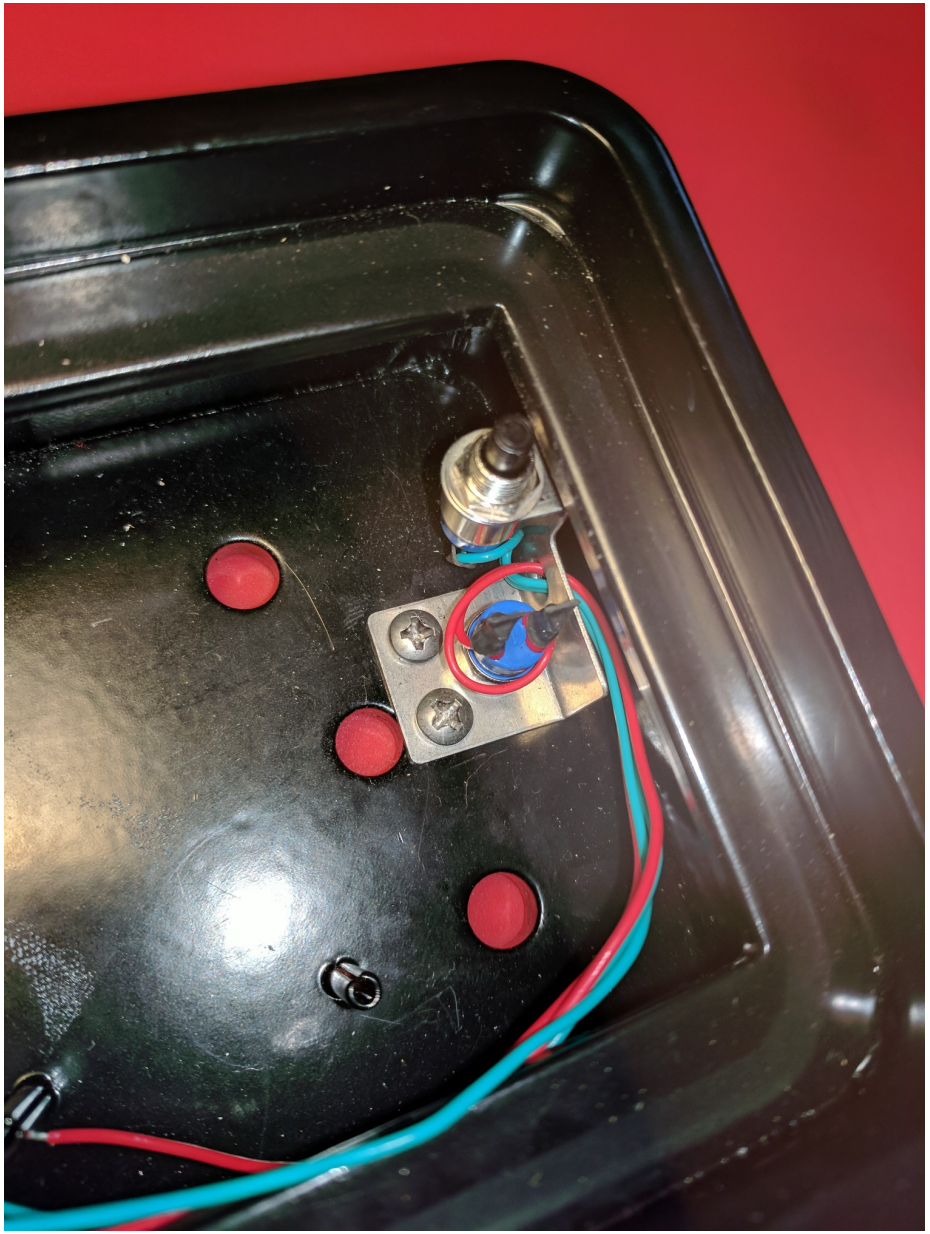
Highly Secure

- AES encrypted
- eLock cores cannot be hacked or detected via RF or Bluetooth technology

Short-term solutions

- Tamper alert

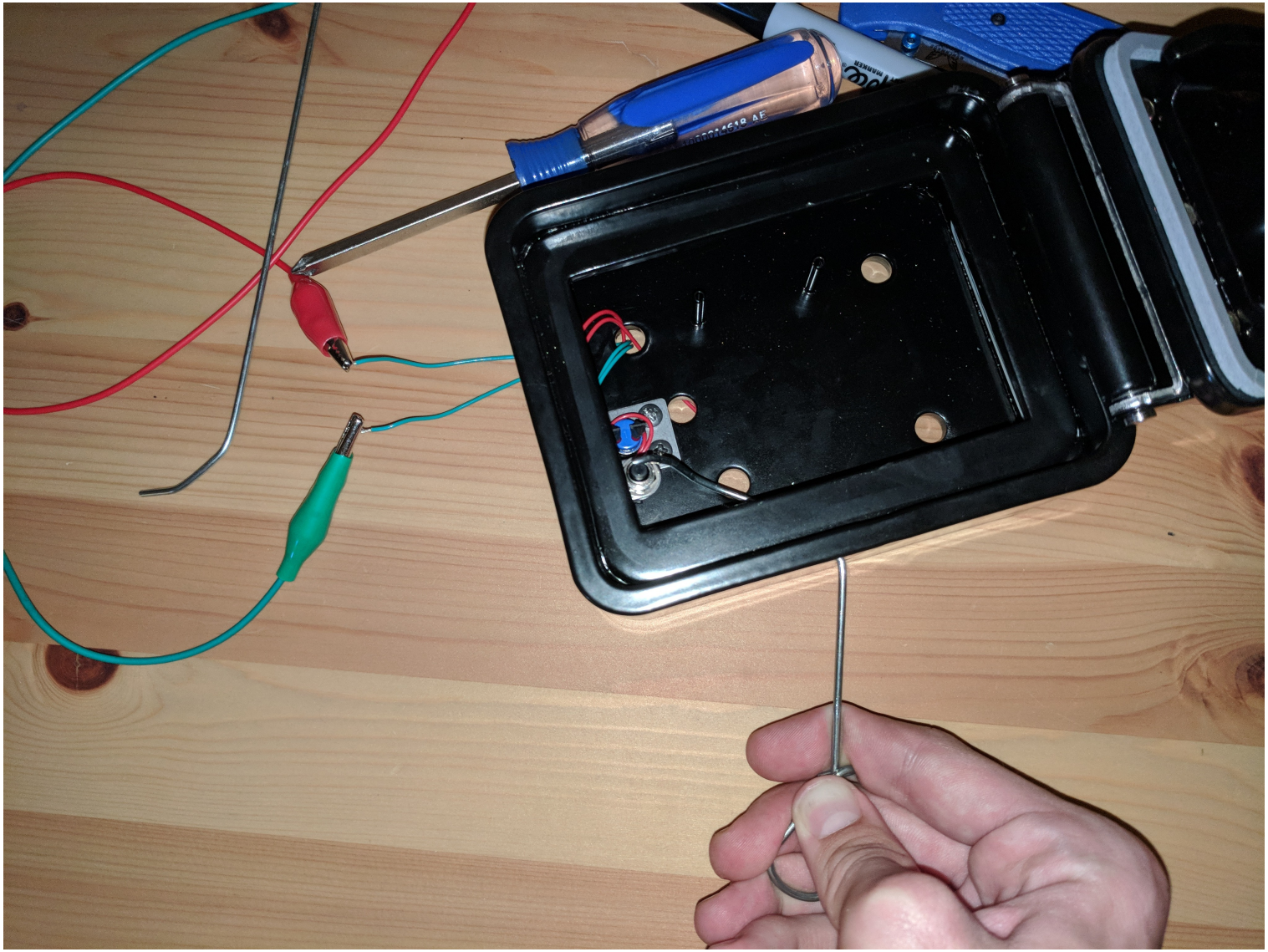
Tamper alert



Tamper alert?



Tampering with the tamper alert



Tampering with the tamper alert



Tampering with the tamper alert



Tampering with the tamper alert



Tampering with the tamper alert



[citation needed]



Highest security when equipped
with optional alarm tamper alert

Short-term solutions

- Tamper alert
  - No drain hole
- Cameras
- Alarm

Long-term solutions

- Switch to a better product lol

Appendix

- github.com/100gamma/Gatekeyper

Thanks





\end{Talk}

@m010ch_
zamak@protonmail.ch
github.com/100gamma/Gatekeyper