Defeating Moving Elements in High Security Keys

Bill Graydon

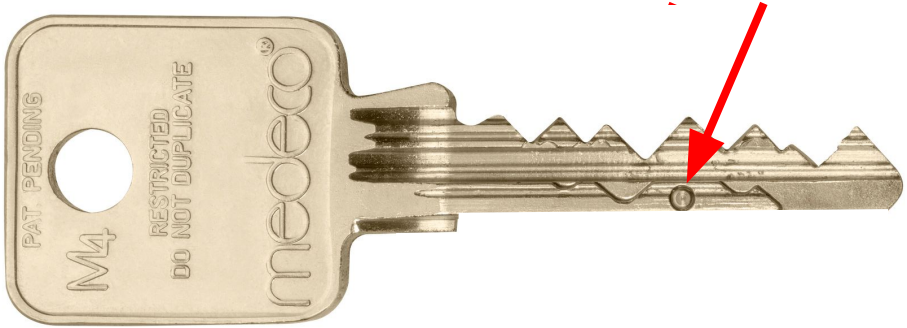
@access_ctrl
b.graydon@ggrsecurity.com
github.com/bgraydon

Outline

- What is a moving element?
- How can we hack them?
  - 3D Print Captive
  - Compliant
  - Static
- Vendor Disclosure
- Implications
- Defenses


MUL-T-LOCK
INTERACTIVE+

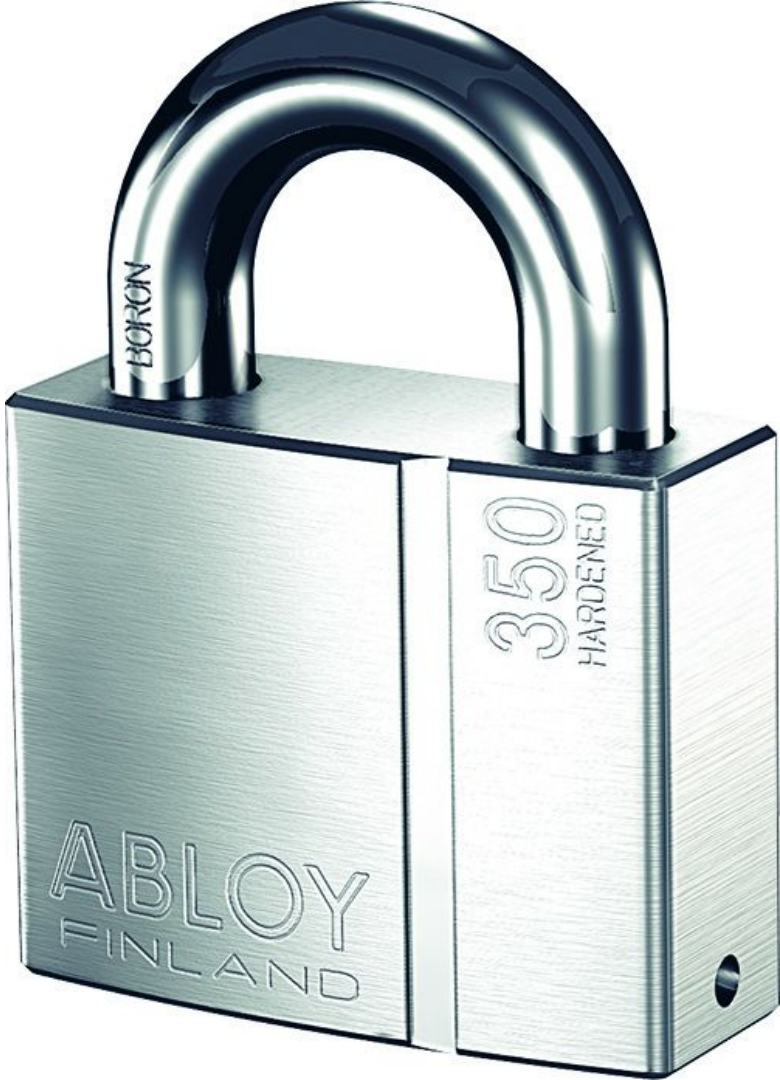

MT5
DO NOT DUPLICATE


PAT PENDING
M4
RESTRICTED
DO NOT DUPLICATE
medeco

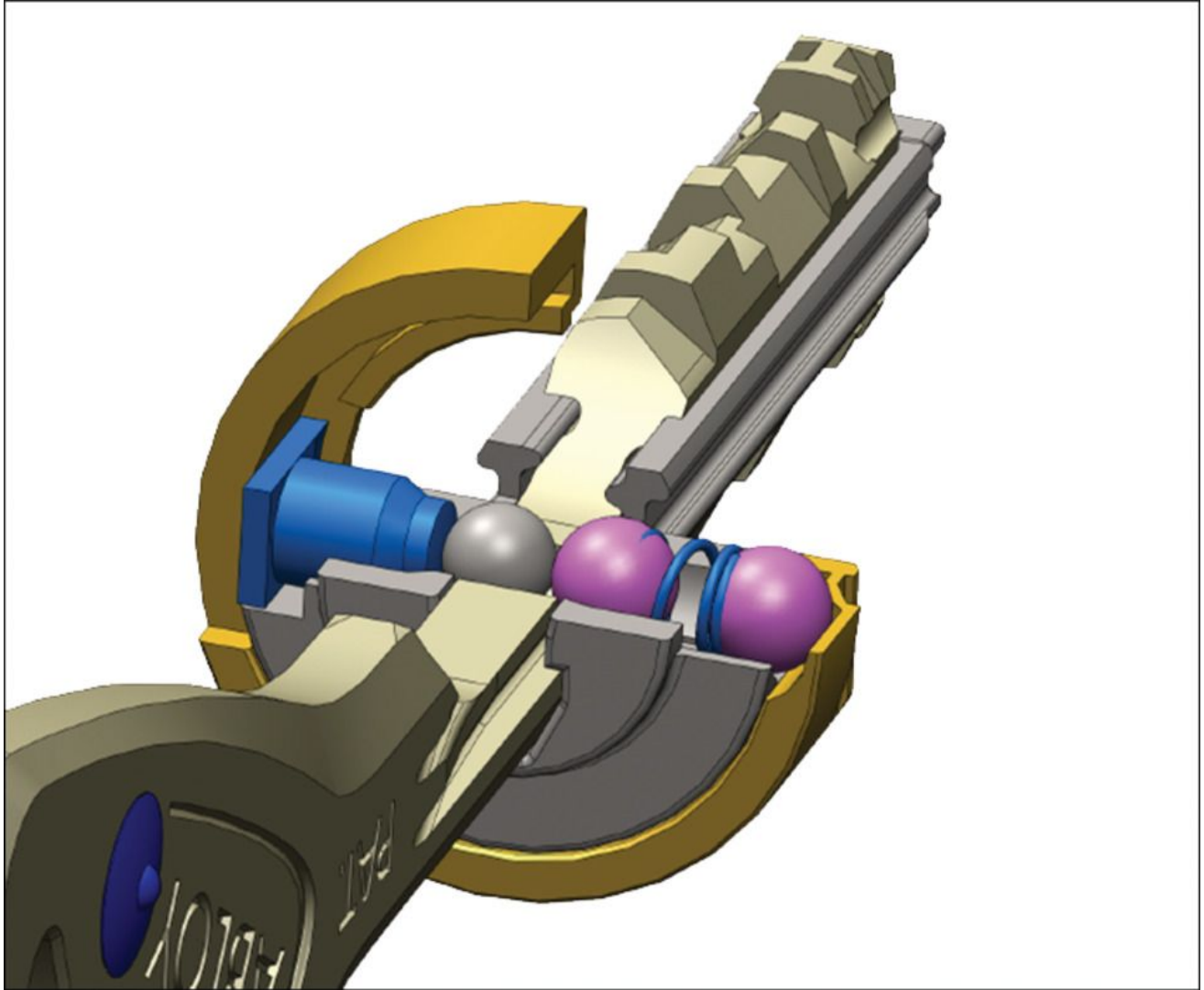

PAT.
ABLOY

Casting


ABLOY
HARDENED


BORON
350
HARDENED
ABLOY
FINLAND

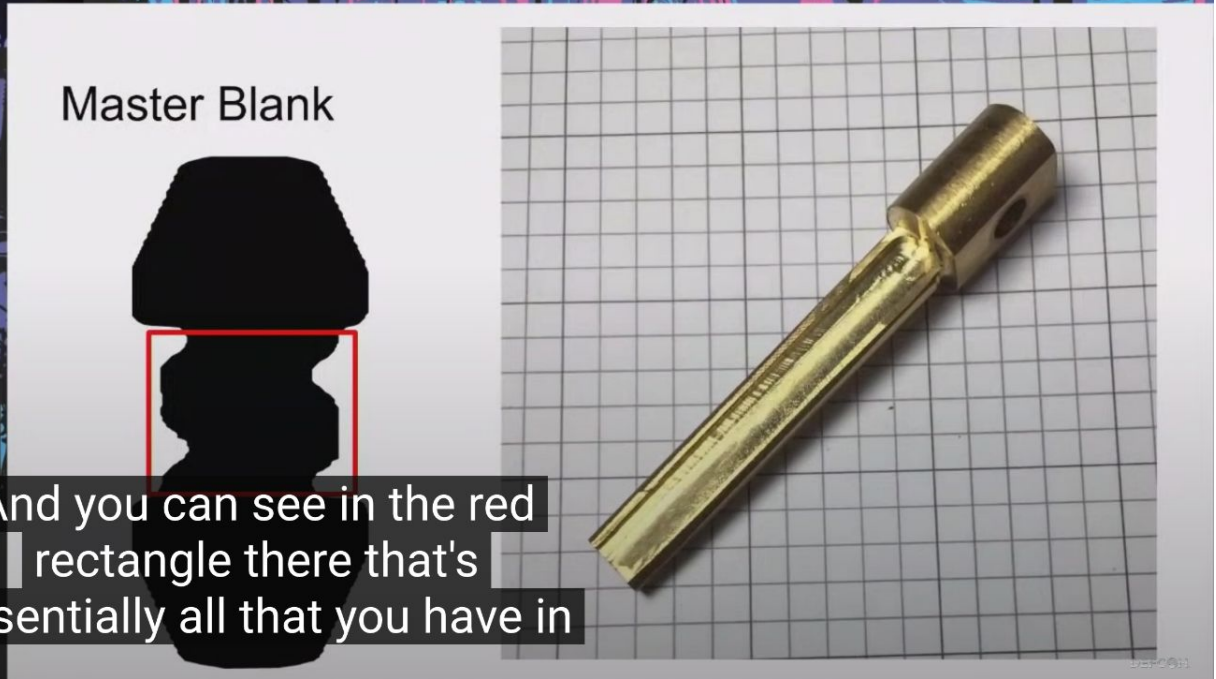

ABLOY
PAT.
PAT.
ABLOY




ABLOY
PAT.
ABLOY
PAT.


ABLOY
ABLOY
PAT.


CRMOLY



And you can see in the red rectangle there that's essentially all that you have in

nvx / protec-3d-printing Public

Watch 7 Fork 10 Star 26

Code Issues Pull requests 1 Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Add file Code

nvx Add tip_cut_all flag to generate a modified tip that sho... 869c3d1 on Sep 23, 2019 4 commits

.gitignore	Add README	3 years ago
README.md	Add tip_cut_all flag to generate a modified tip that shoul...	3 years ago
protec.scad	Add tip_cut_all flag to generate a modified tip that shoul...	3 years ago

README.md

Parametrically Generated 3D Printable ABLOY PROTEC Keys

Inspired by Dave Pedu's 3D printed Kwikset keys and that the patents for the ABLOY PROTEC keys were set to expire in a couple of weeks, this OpenSCAD model generates keys for the

About

An OpenSCAD library for parametrically generating ABLOY PROTEC keys suitable for 3D printing

hackaday.io/project/167726-protec-3d-p...

Readme

26 stars

7 watching

10 forks

Releases

No releases published

Packages

bgraydon / abloy-protec2-3d-printing

Public

forked from nvx/protec-3d-printing

master | 1 branch | 0 tags | Go to file | Add file | Code

This branch is 2 commits ahead of nvx:master. | Contribute | Sync fork

Bill Graydon	Added first draft of captive, compliant, and static optio...	e064a09	4 hours ago	6 commits
.gitignore	Add README		3 years ago
README.md	Add tip_cut_all flag to generate a modified tip that shoul...		3 years ago
protec.scad	Added first draft of captive, compliant, and static options...		4 hours ago

README.md

Parametrically Generated 3D Printable ABLOY PROTEC Keys

About

An OpenSCAD library for parametrically generating ABLOY PROTEC2 keys suitable for 3D printing

hackaday.io/project/167726-protec-3d-p...

Readme

0 stars

0 watching

10 forks

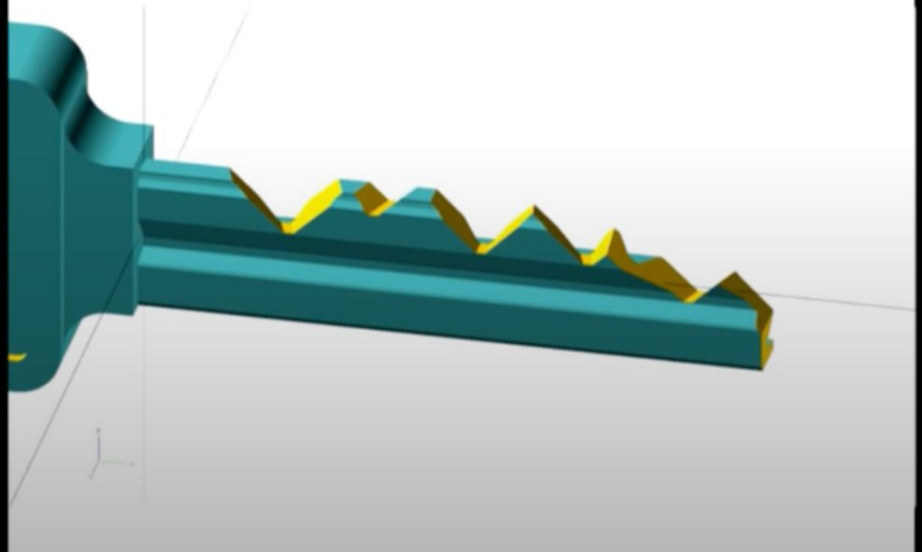
Releases

No releases published

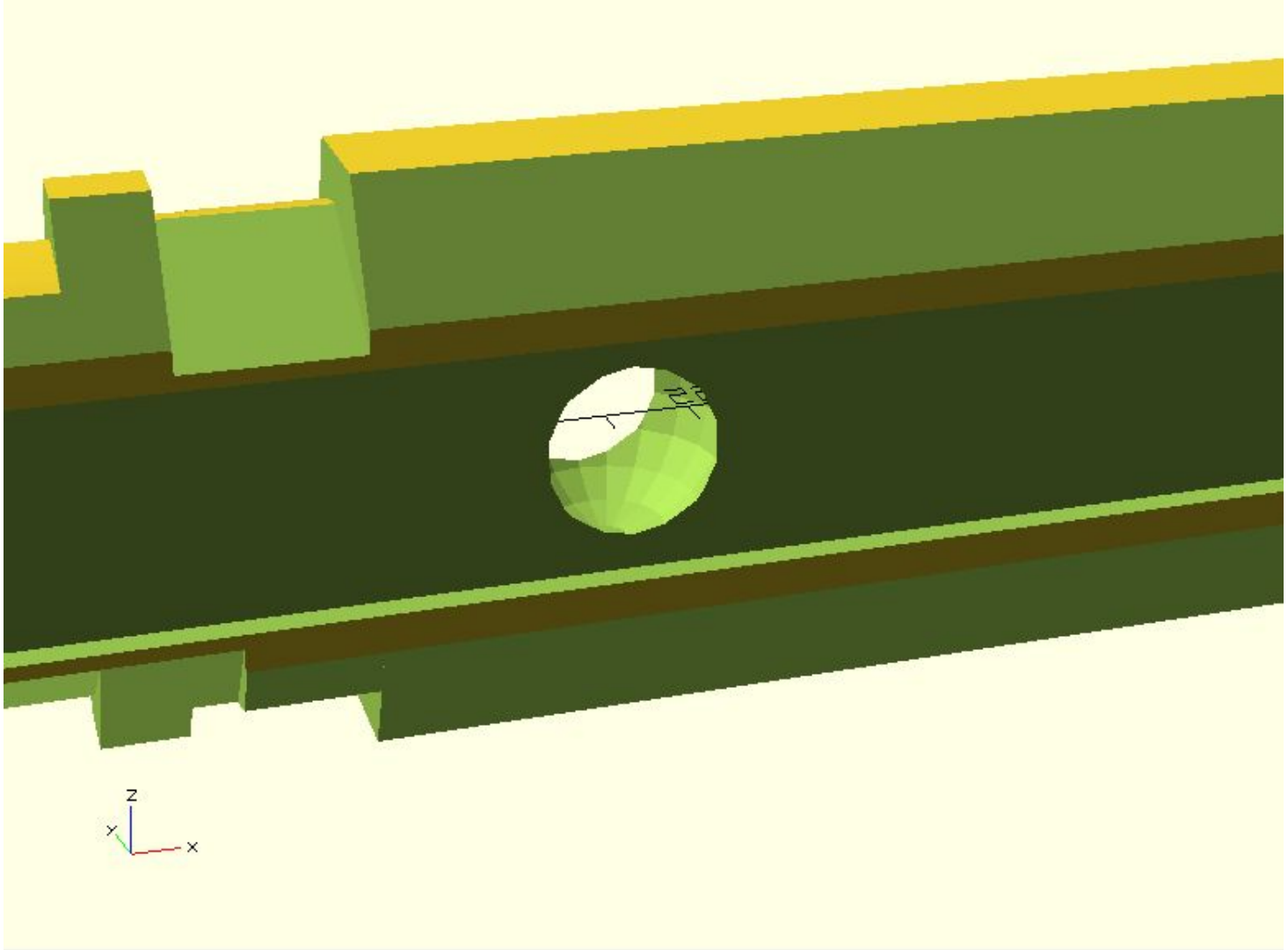
Create a new release

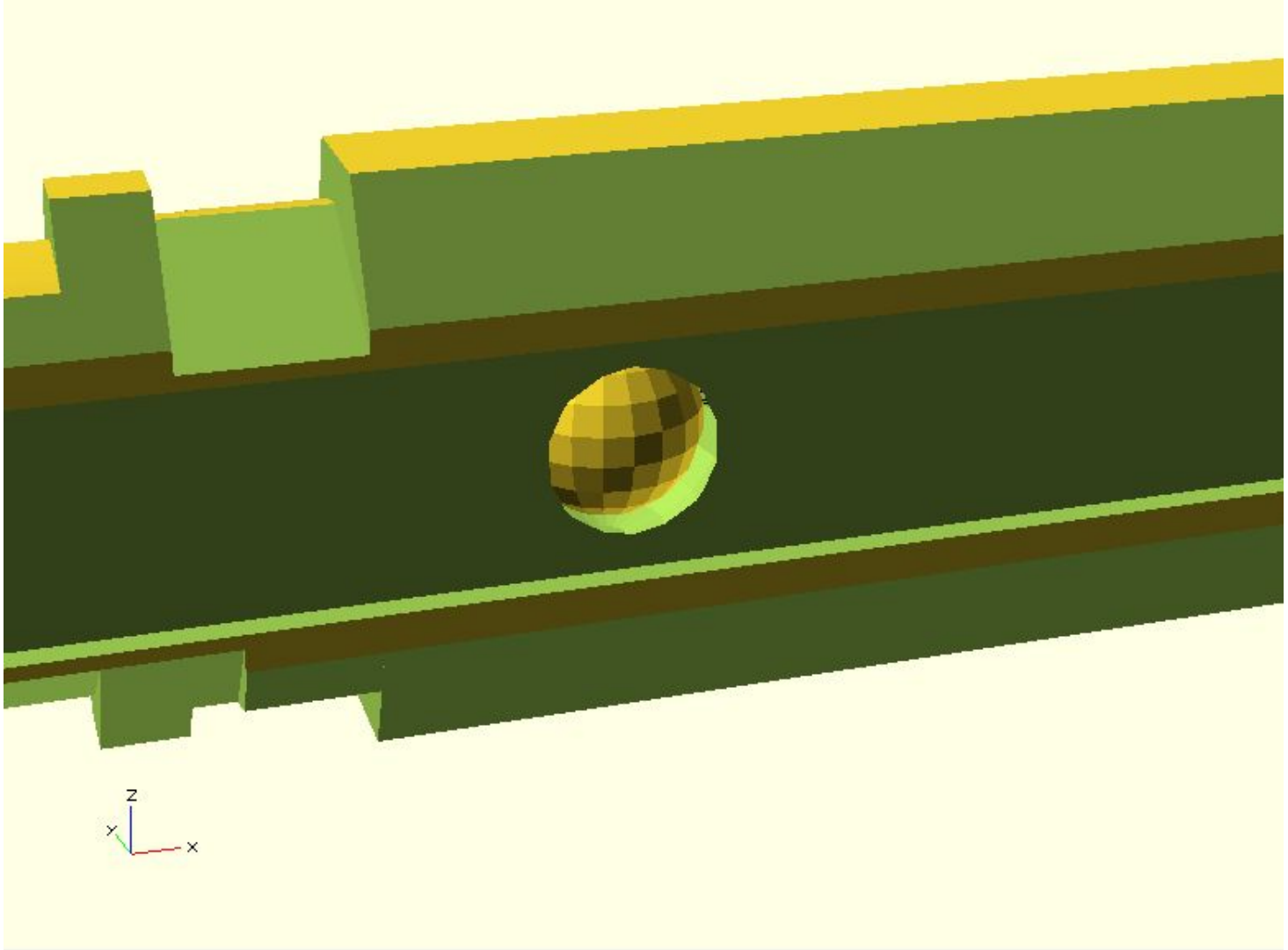
DEFCON

Modeling the cuts

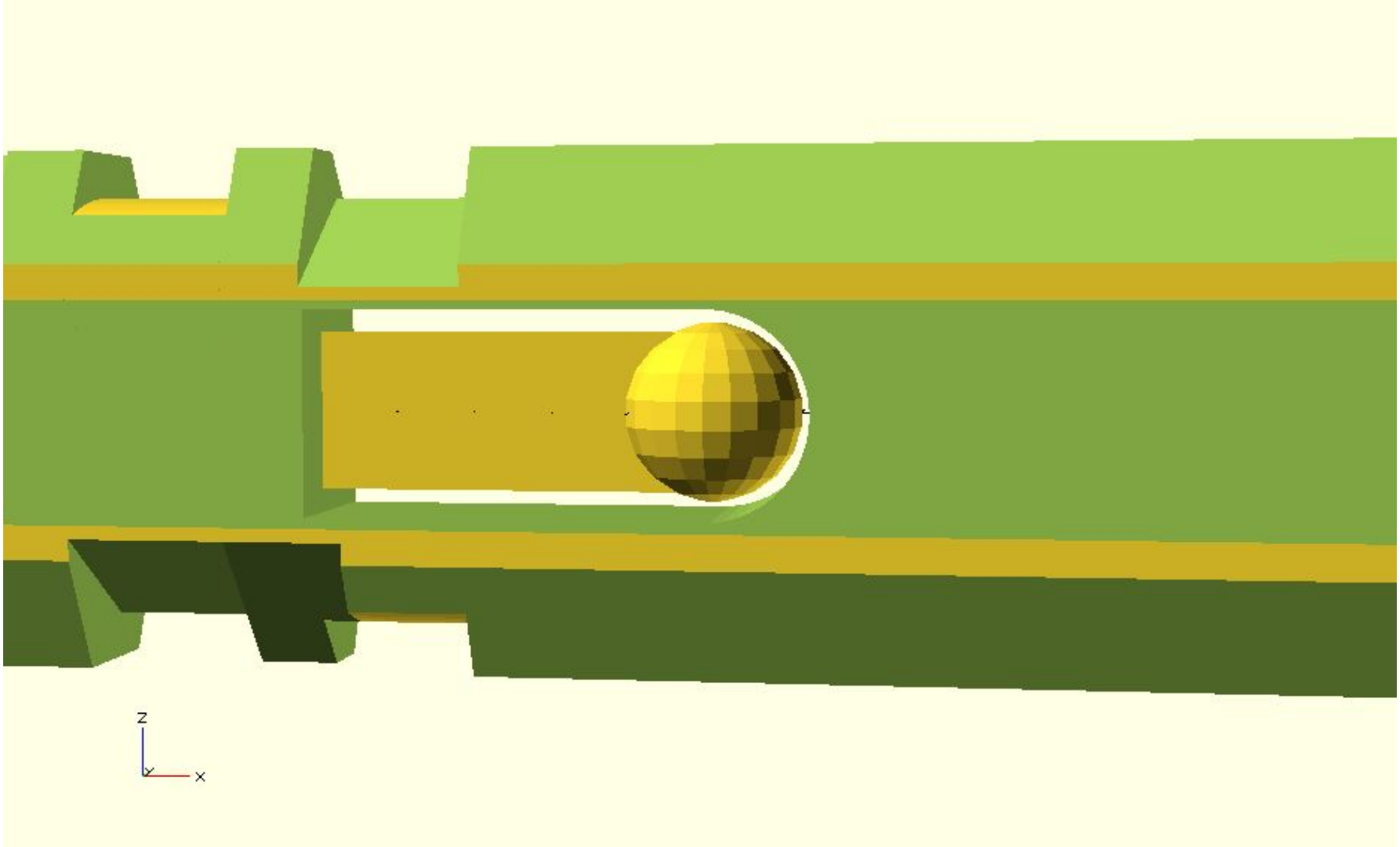


AUGUST 9-12, 2018
LAS VEGAS

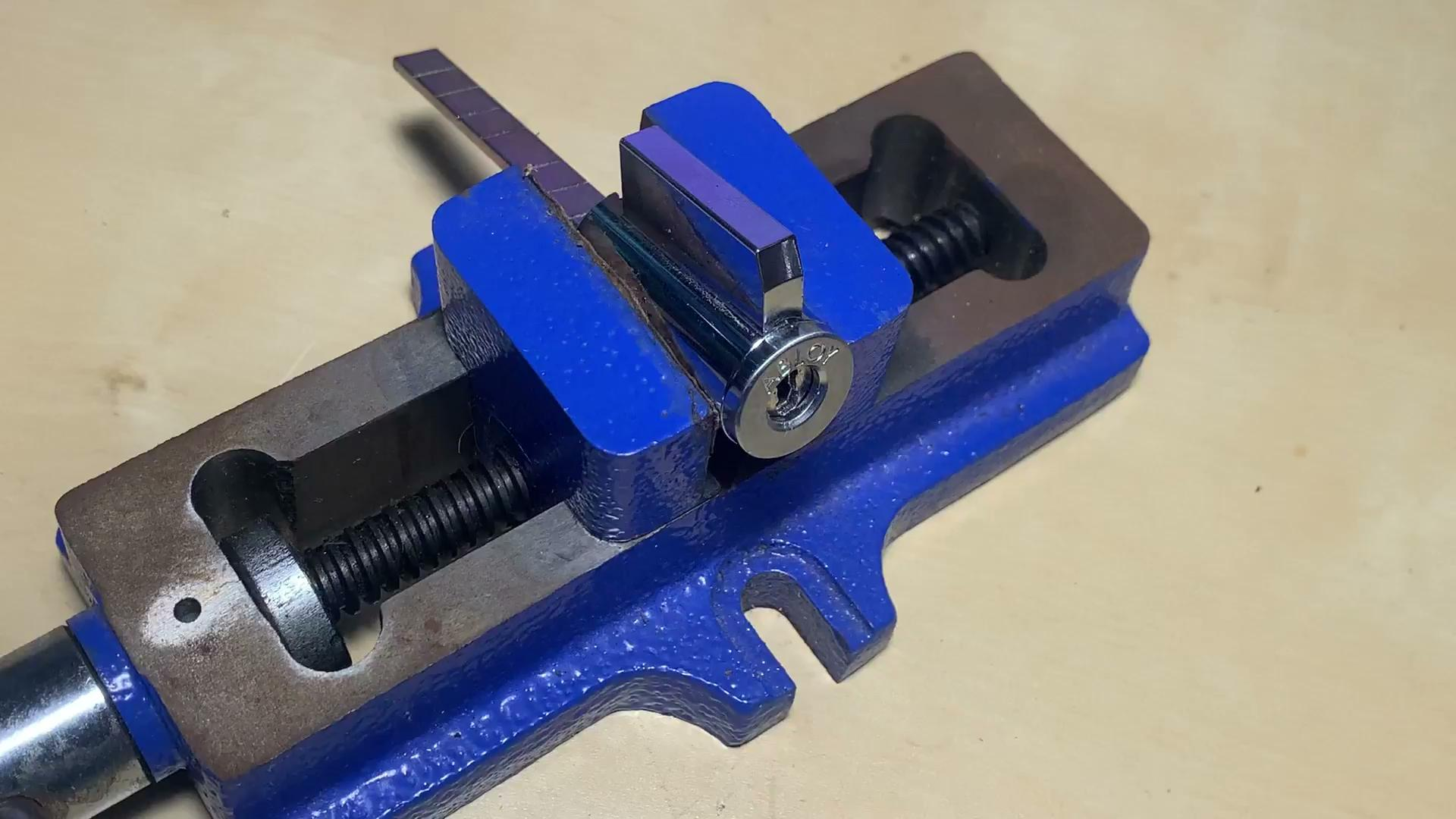

Z
Y
X


Z
Y
X


cpt 1.3
cpt 1.4
cpt 1.5
cpt 1.6
cpt 1.7
cpt 1.8
cpt 1.9
cpt 2.0
cpt 2.1


z
x


ABLOY
PAT.



Exploiting Keyspace Vulnerabilities in Locks

Bill Graydon

@access_ctrl
b.graydon@ggrsecurity.com
github.com/bgraydon

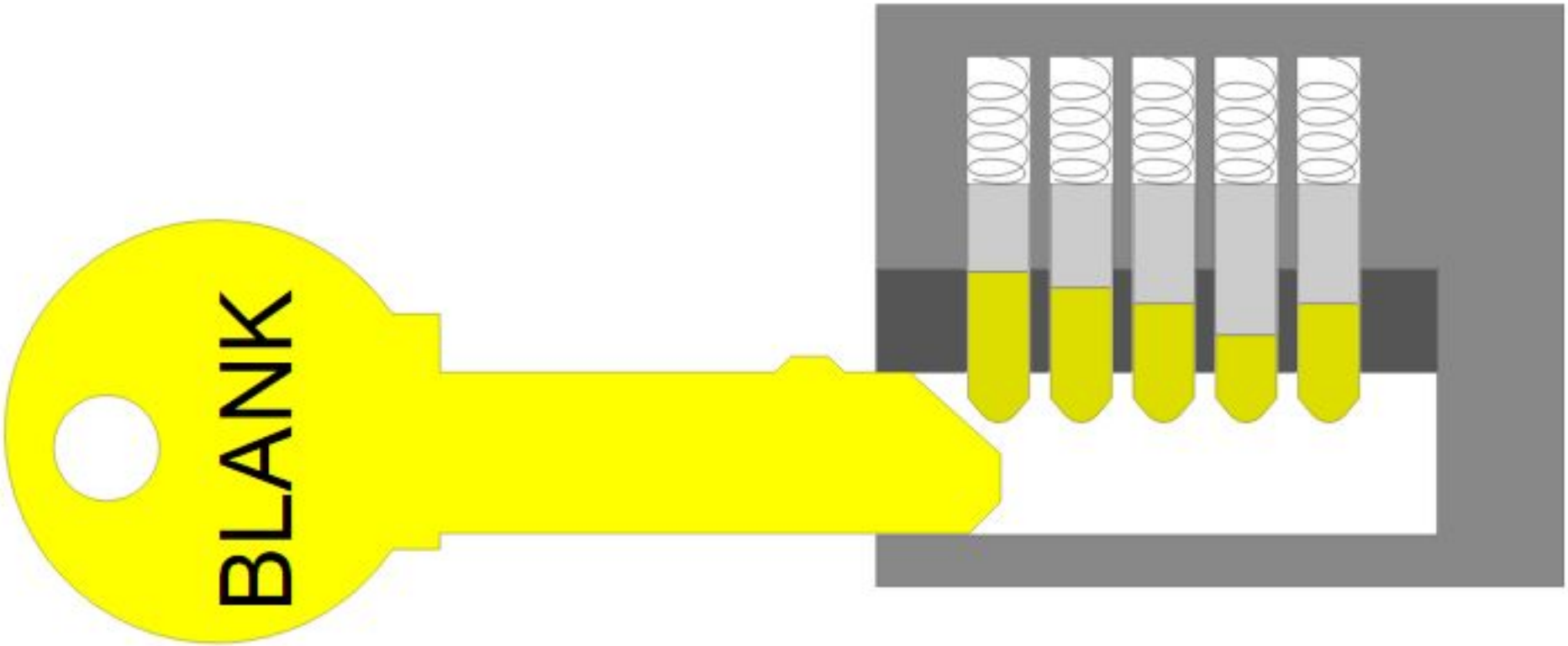
GGR
SECURITY CONSULTANTS

in the Physical World | Bill Graydon | Exploiting

DEF CON SAFE MODE
TALKS

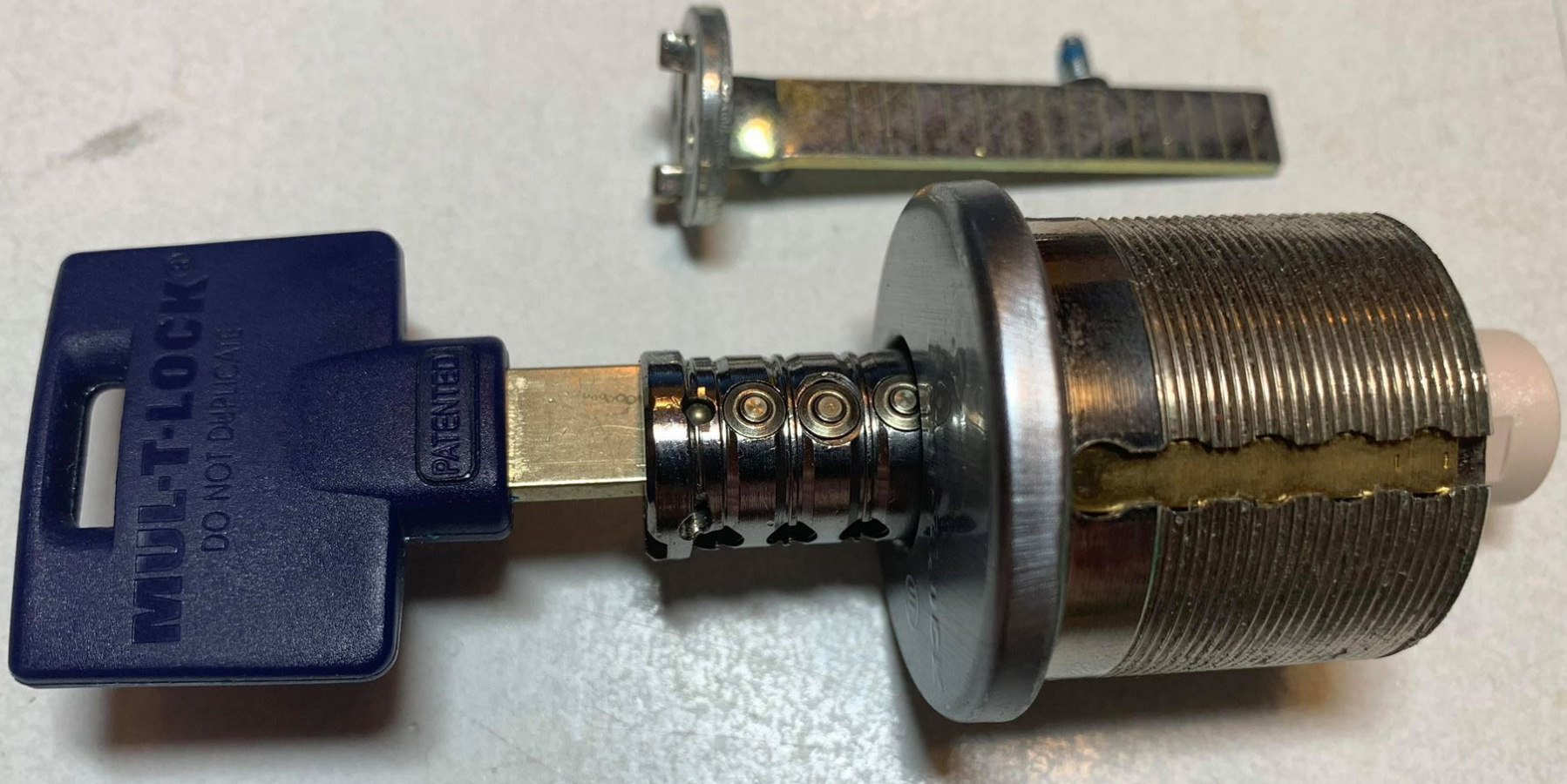
DEF CON ACTUALLY CANCEL

DEFCON

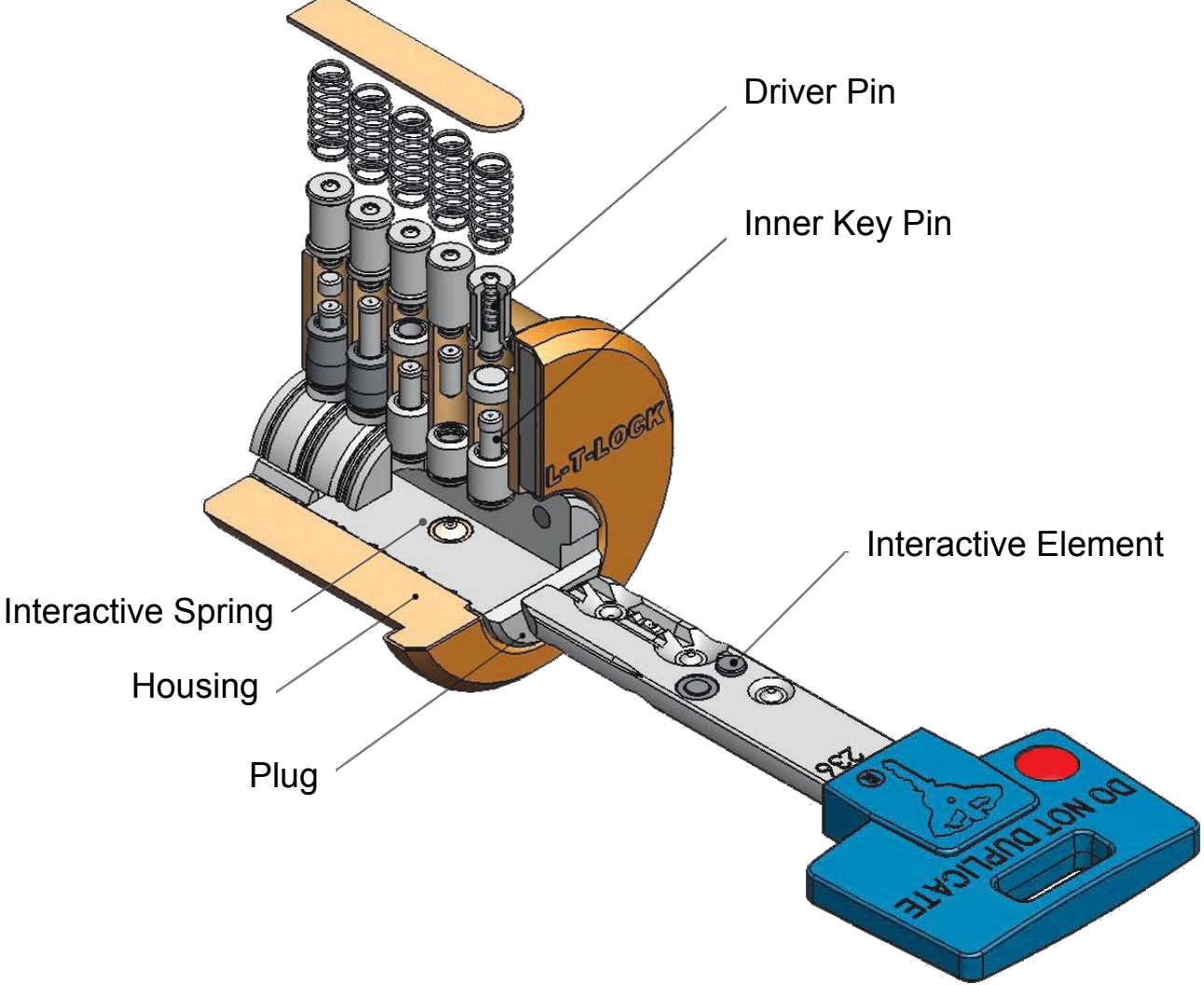

BLANK


MUL-T-LOCK
UL

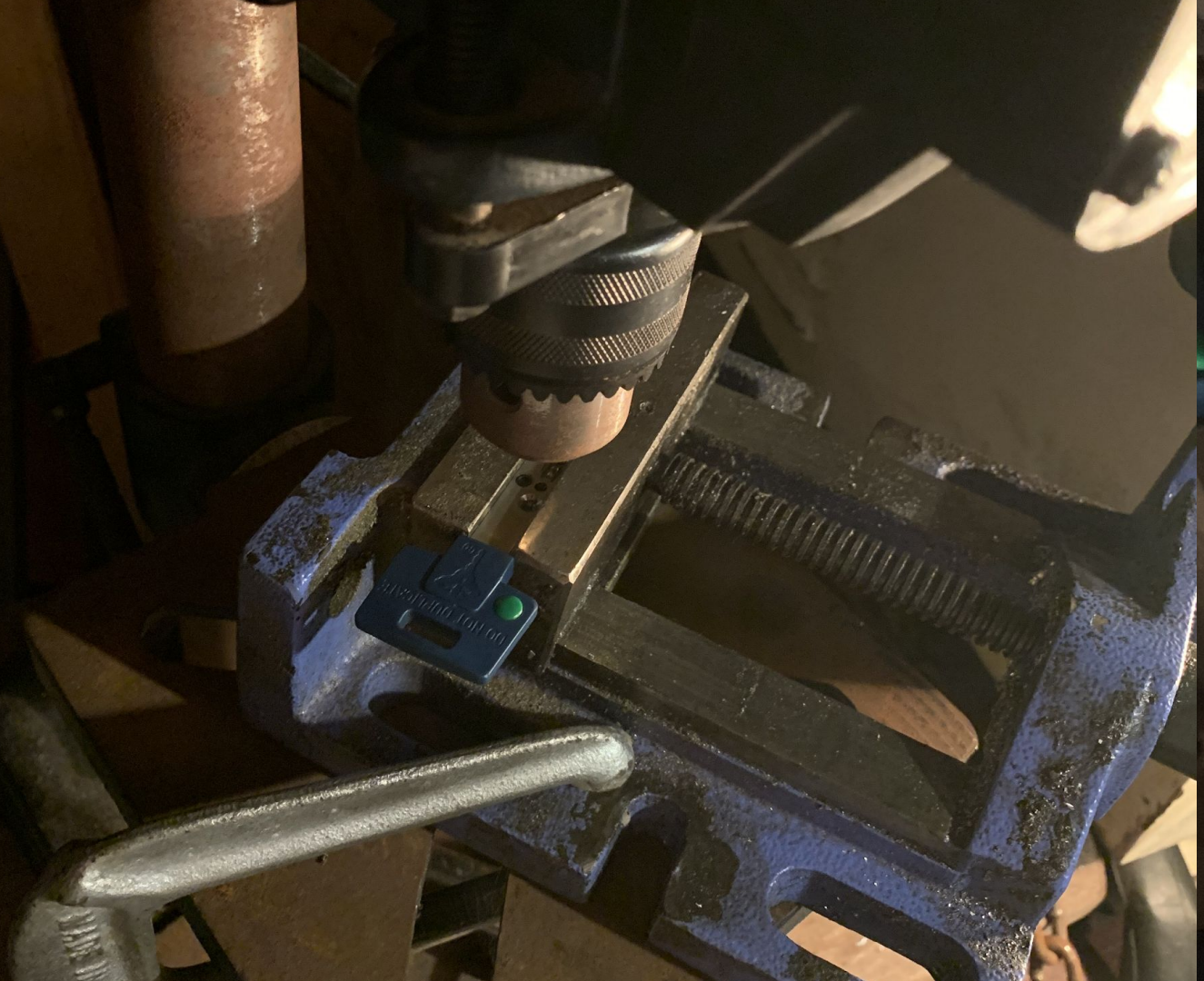

MUL-T-LOCK


MUL-T-LOCK®
DO NOT DUPLICATE
PATENTED

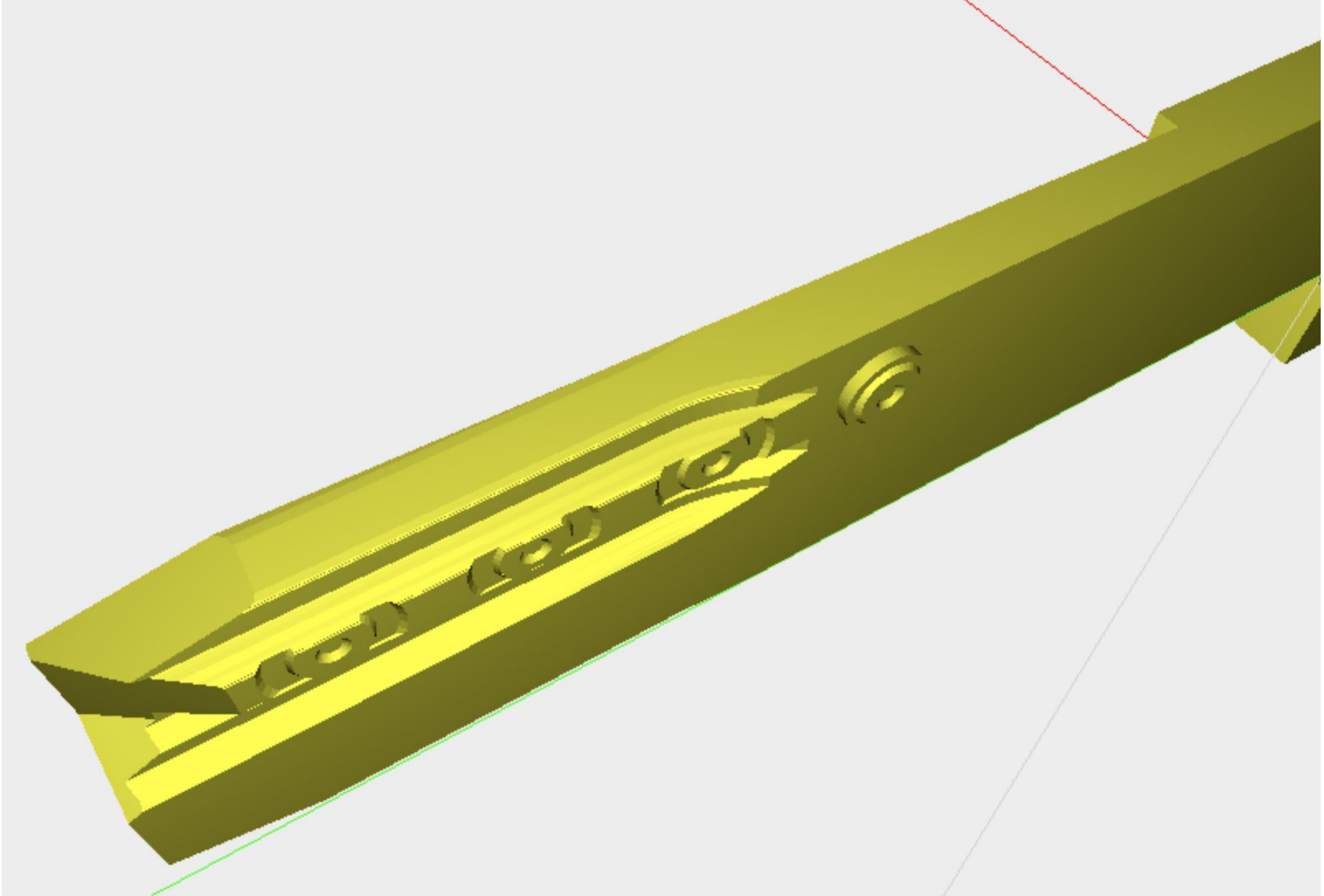

MUL-T-LOCK
INTERACTIVE+
DO NOT DUPLICATE
MT5


Driver Pin
Inner Key Pin
Interactive Element
Interactive Spring
Housing
Plug
L-T-LOCK
DO NOT DUPLICATE


Mastercraft



264
MUL-T-LOCK®
PATENTED
264



Mul-T-Lock 006C Classic Key blank

(No reviews yet) Write a Review

SKU: 39486

MPN: 006C-KEYBLK

BULK DISCOUNT RATES

Below are the available bulk discount rates for each individual item when you purchase a certain amount

Buy 1 - 9	and pay only $6.94 each
Buy 10 - 49	and pay only $3.26 each
Buy 50 or above	and pay only $2.60 each

$6.94

CURRENT STOCK: 70

QUANTITY:

1

ADD TO CART

Key tool B316 Home Door Key blanks Locksmith Supplies Blank Keys 20 pieces/lot

★★★★★ 5.0 3 Reviews 5 orders

US $12.25 / lot (20 Pieces)

~~US $12.90~~ -5%

US $3.00 off Coupons For You Get coupons

Quantity: 1 959 lots available

Ships to United States

Shipping: $1.60

From China to United States via AliExpress Standard Shipping

Estimated delivery on Aug 17 More options

Buy Now Add to Cart ♡ 22

75-Day Buyer Protection
Money back guarantee

Free Return
Return for any reason within 15 days

Recommended For You

US $12.06

US $2.03

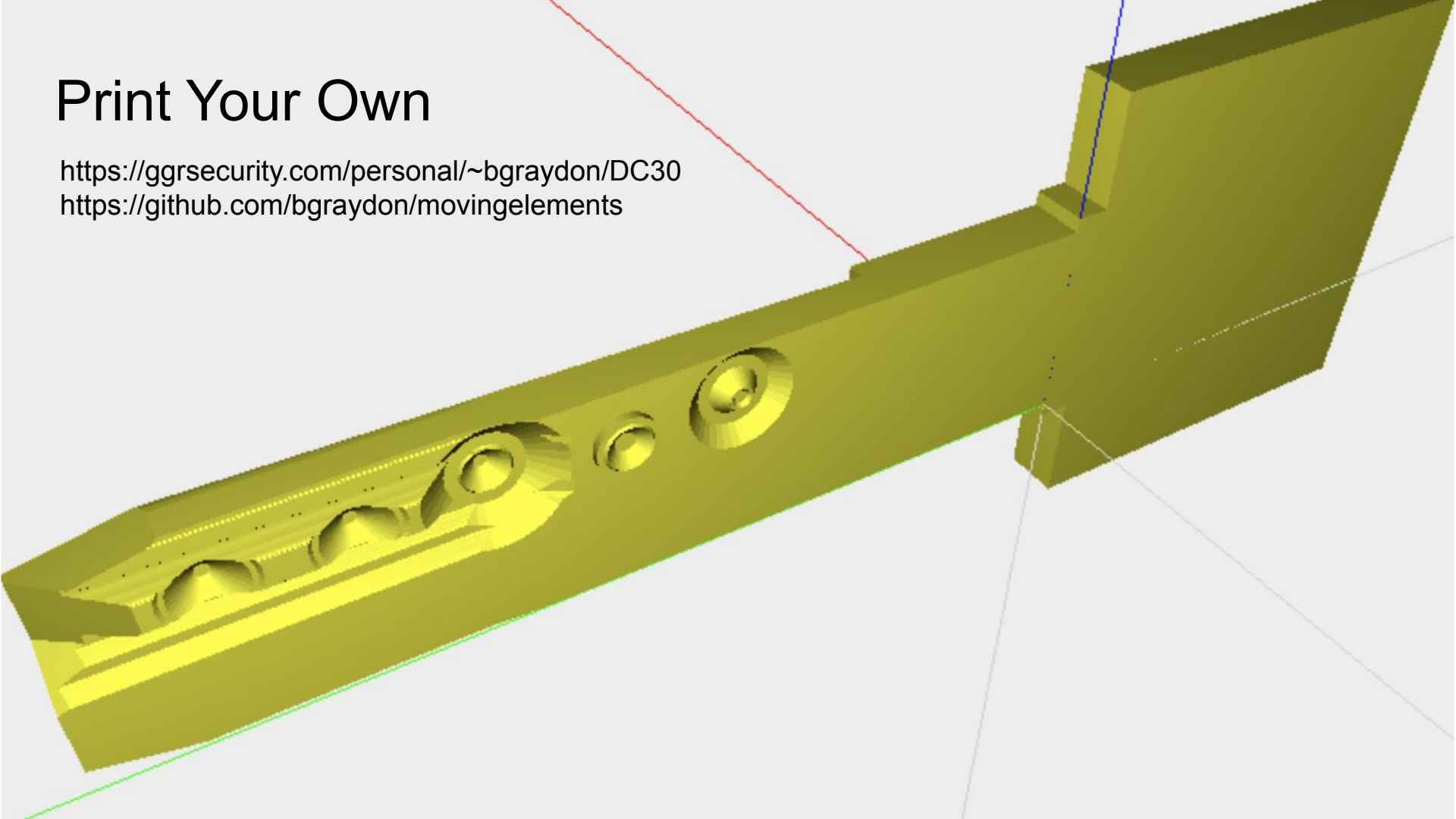
US $13.77


MUL-T-LOCK®
DO NOT DUPLICATE
PATENTED


ABUS
EVOLOCK

Print Your Own

https://ggrsecurity.com/personal/~bgraydon/DC30
https://github.com/bgraydon/movingelements



U.S. Patents Last 20 Years

U.S. Patent Aug. 15, 1989 Sheet 1 of 2 4,856,309

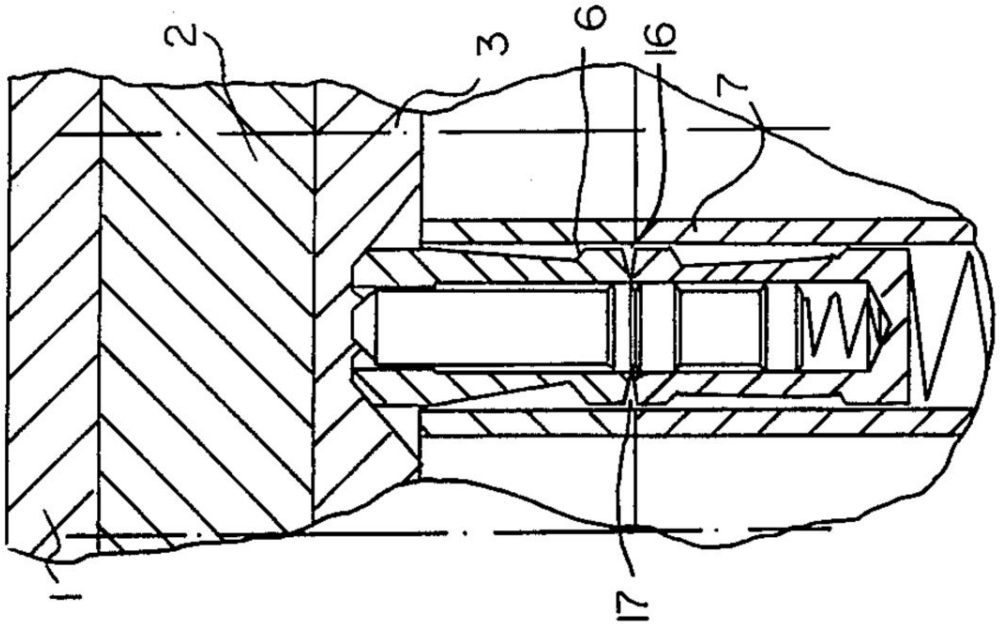


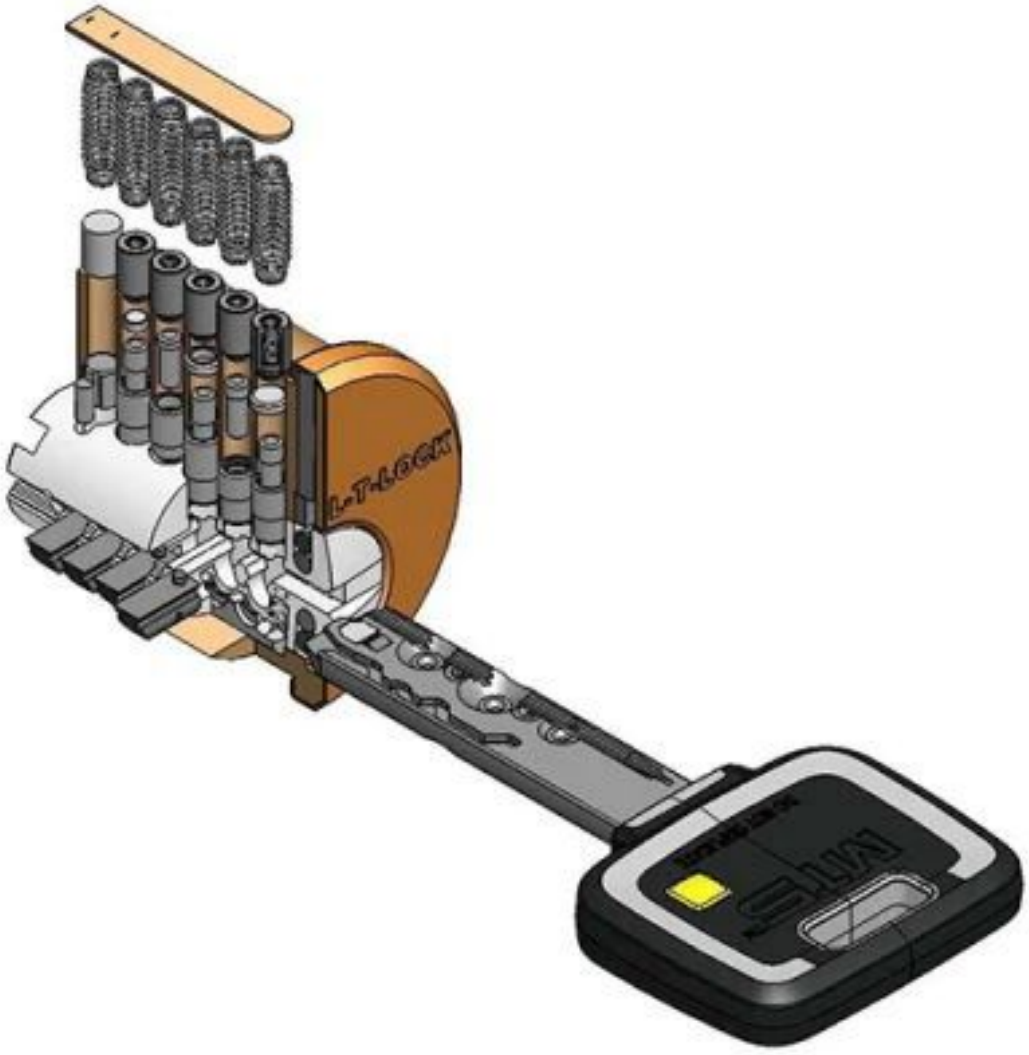
FIG. 2
PRIOR ART

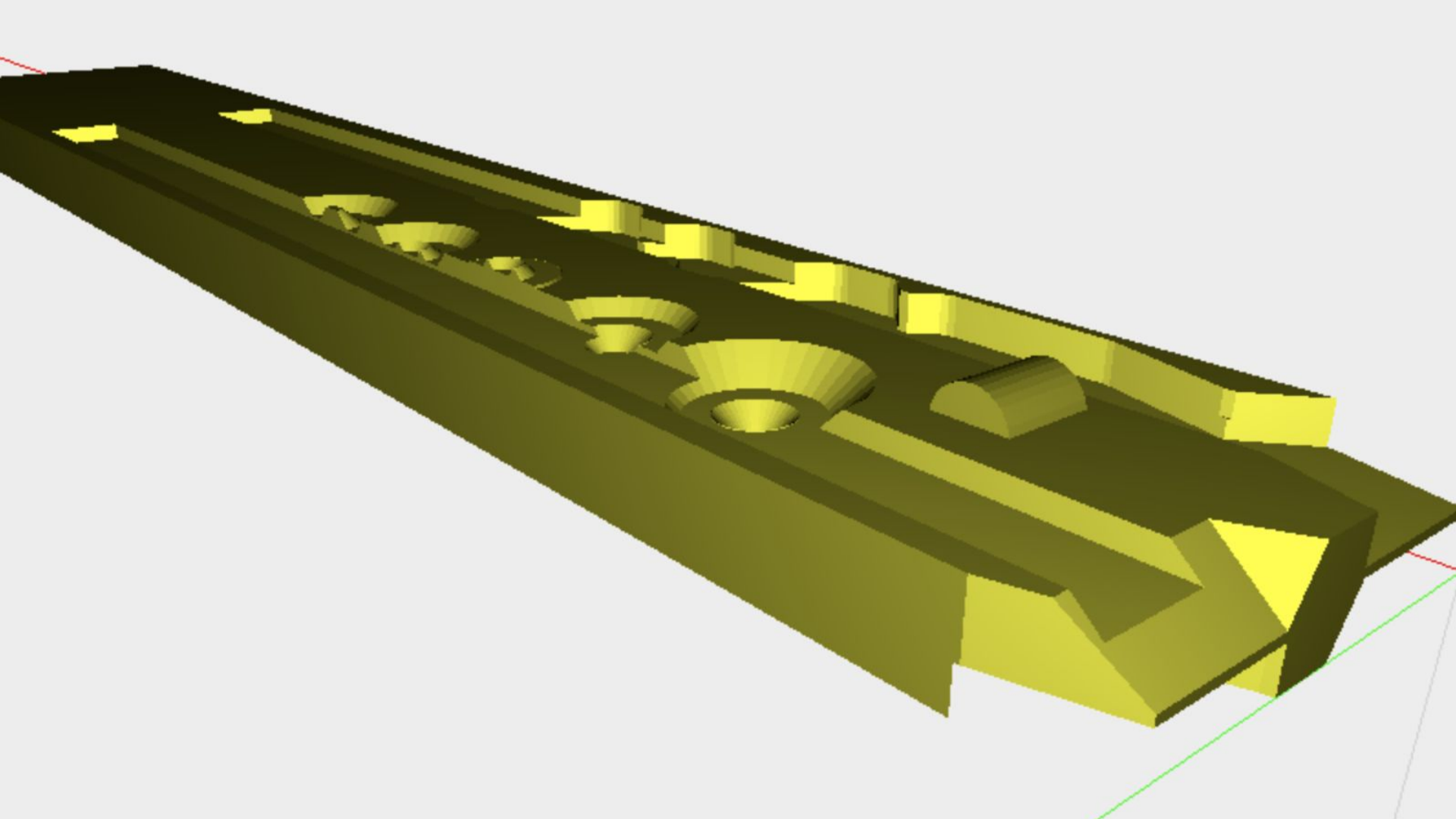
1977

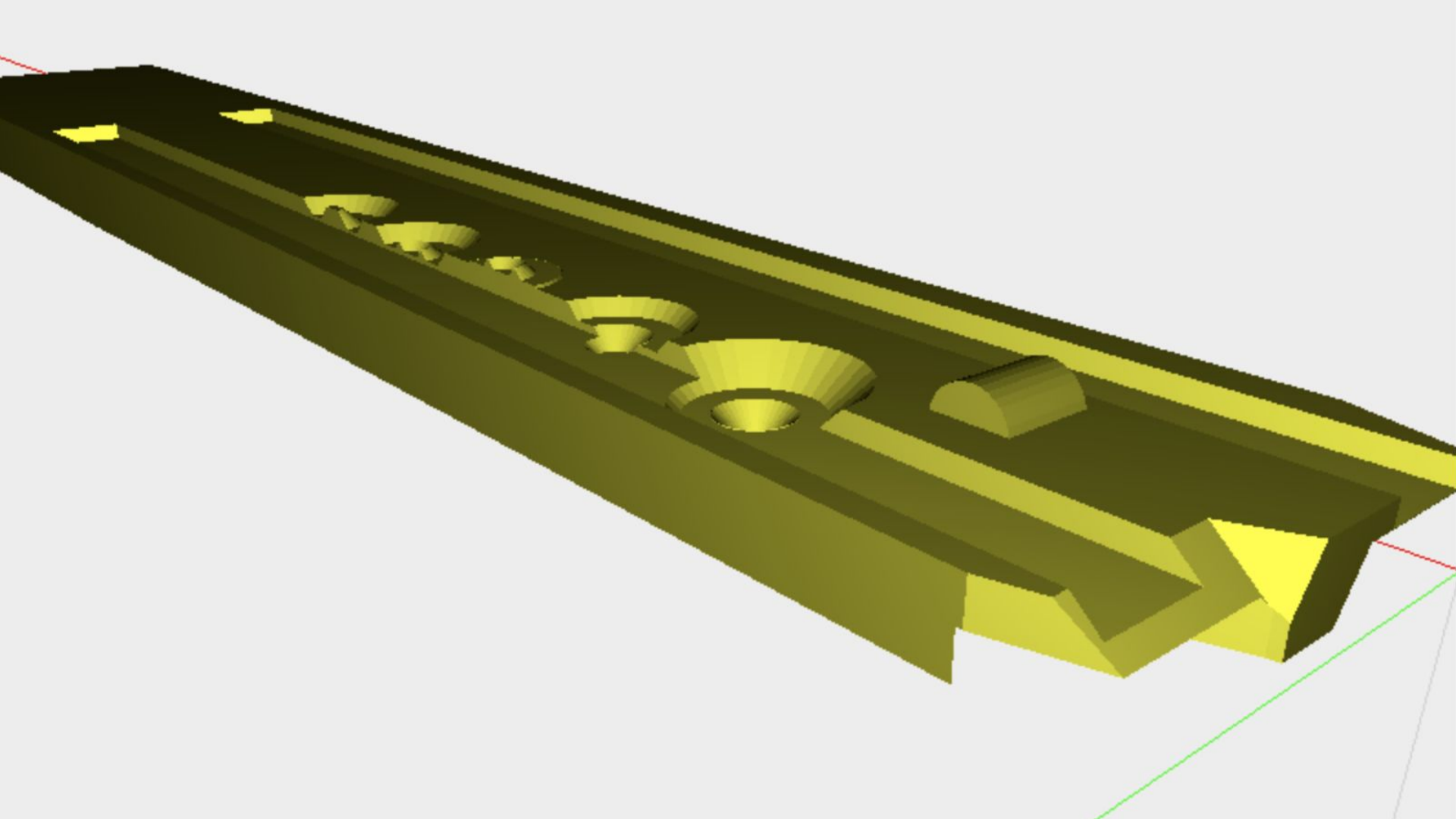
1994

2007

Mul-T-Lock MT5

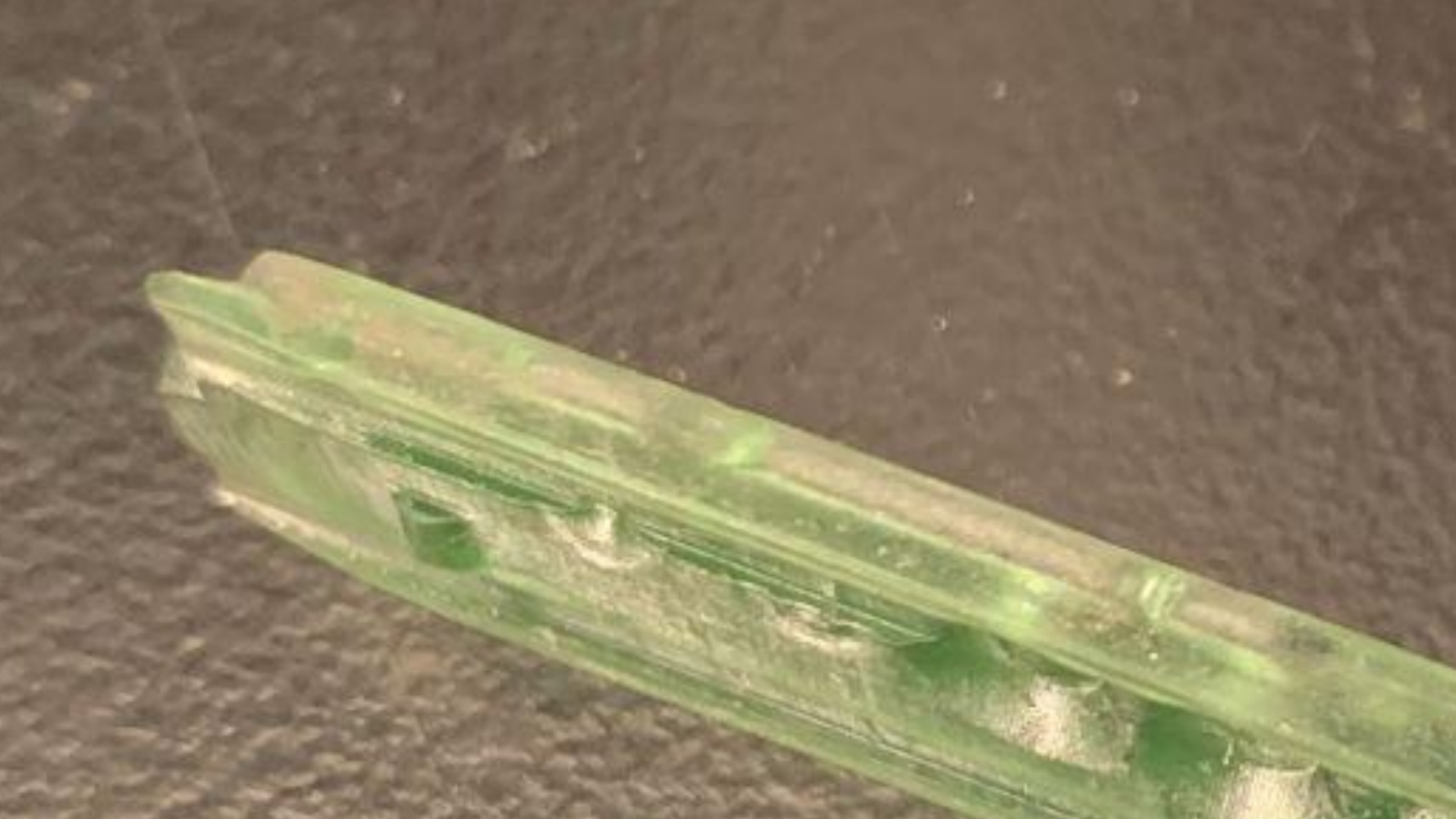

L-T-LOCK

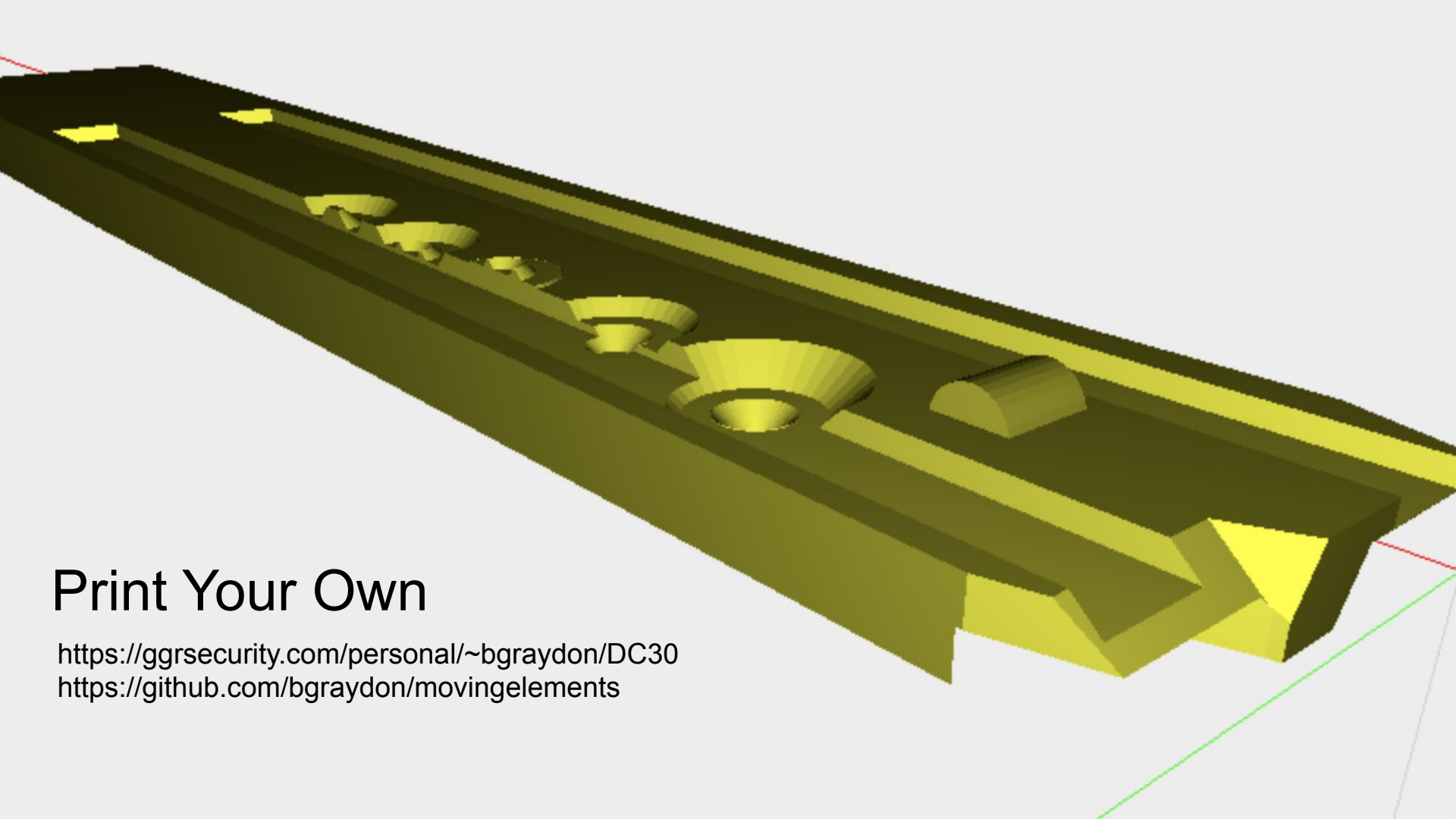





MTE
DO NOT DUPLICATE


MTS®
DO NOT DUPLICATE
5





Print Your Own

https://ggrsecurity.com/personal/~bgraydon/DC30
https://github.com/bgraydon/movingelements

Vendor Outreach

Vulnerability Disclosure in Interactive Key Control

To info@mul-t-lock.com Date 2020-12-29 09:59

Hi folks,

I hope you're doing well! I'd like to reach out to disclose a vulnerability we've discovered in the key control of Mul-T-Lock systems; namely, a means to defeat the interactive component of the Interactive and MT5 models by creating a key which operates the lock out of a single solid piece of material (including by 3D printing).

Please forward this to the appropriate department so I can forward drawings on the technique and we can discuss further. We'd like to assist you in any way we can to mitigate these risks.

In order to keep end users and facility managers appraised of potential threat vectors to their key control, we plan to present this research publicly, tentatively in the summer of 2021. We're reaching out now to give you an opportunity to mitigate these vulnerabilities before we release them to the public.

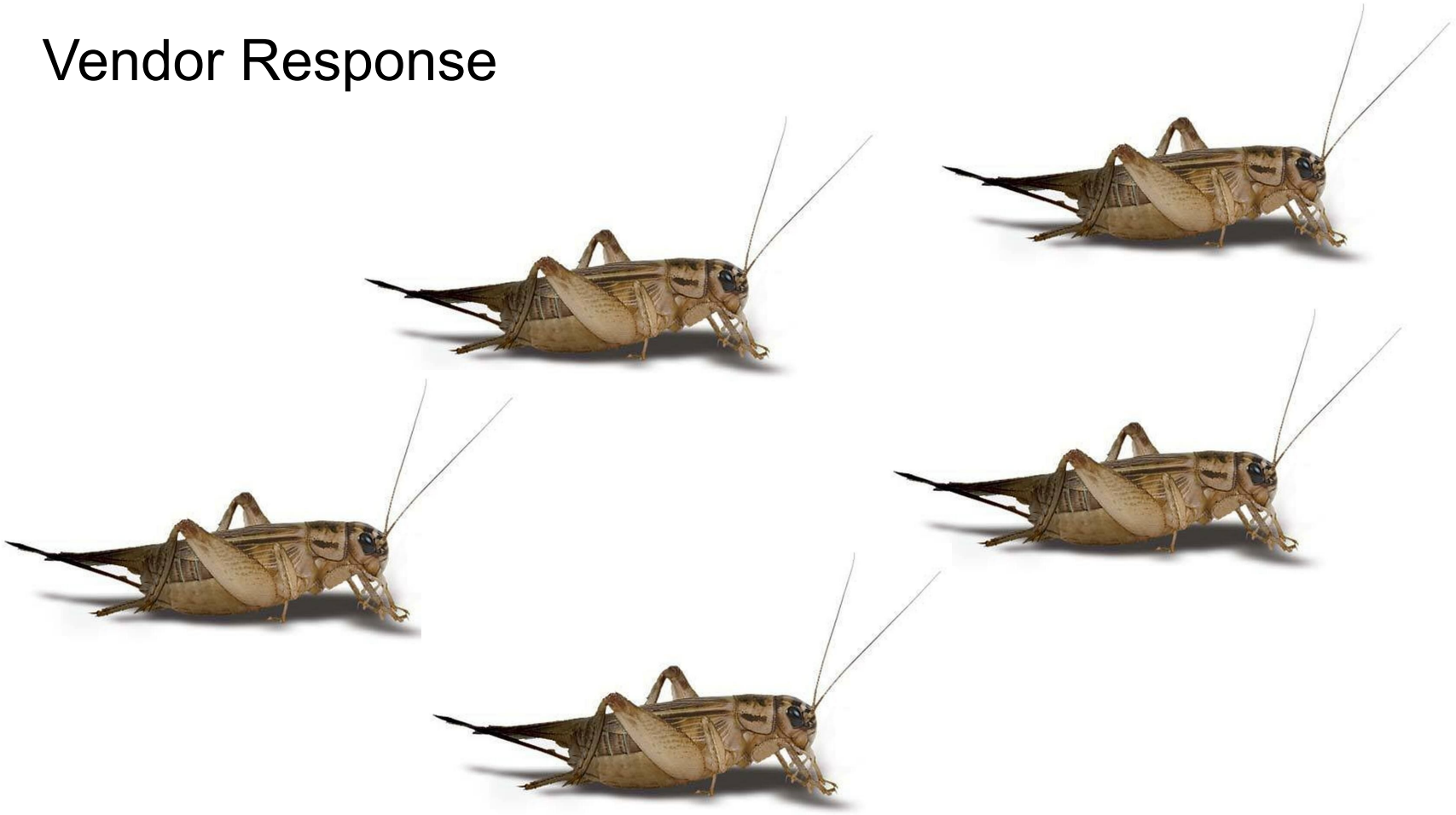
Looking forward to hearing back from you - all the best,

--

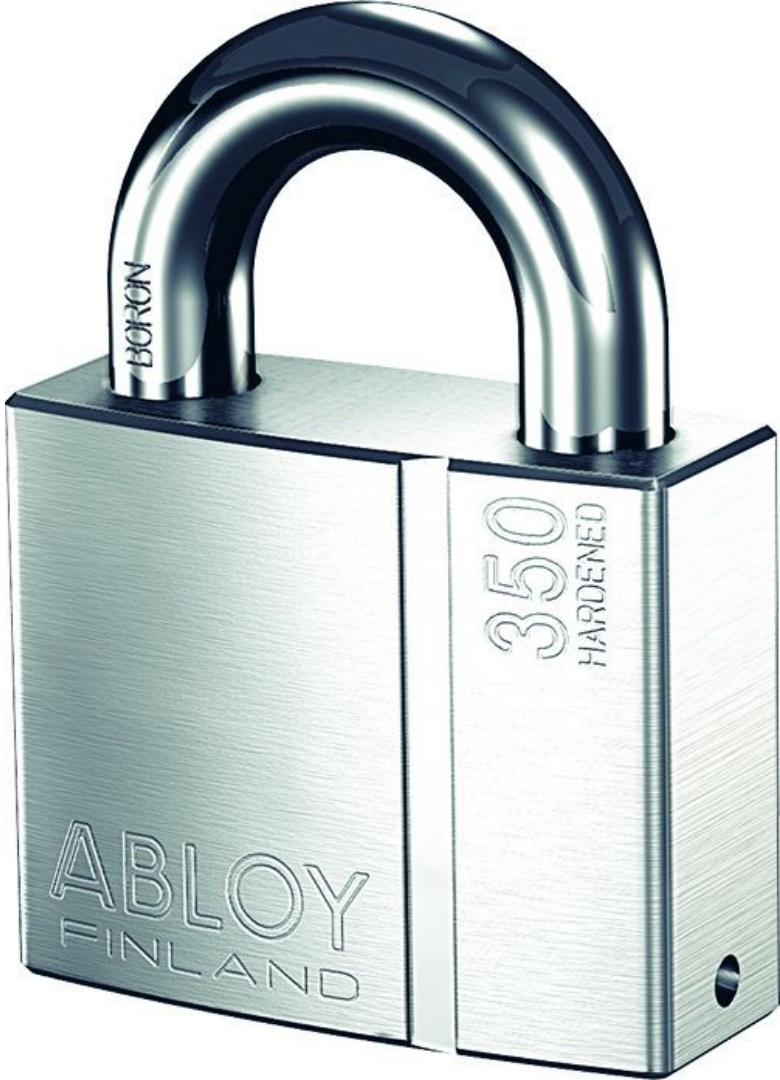
GGR SECURITY CONSULTANTS

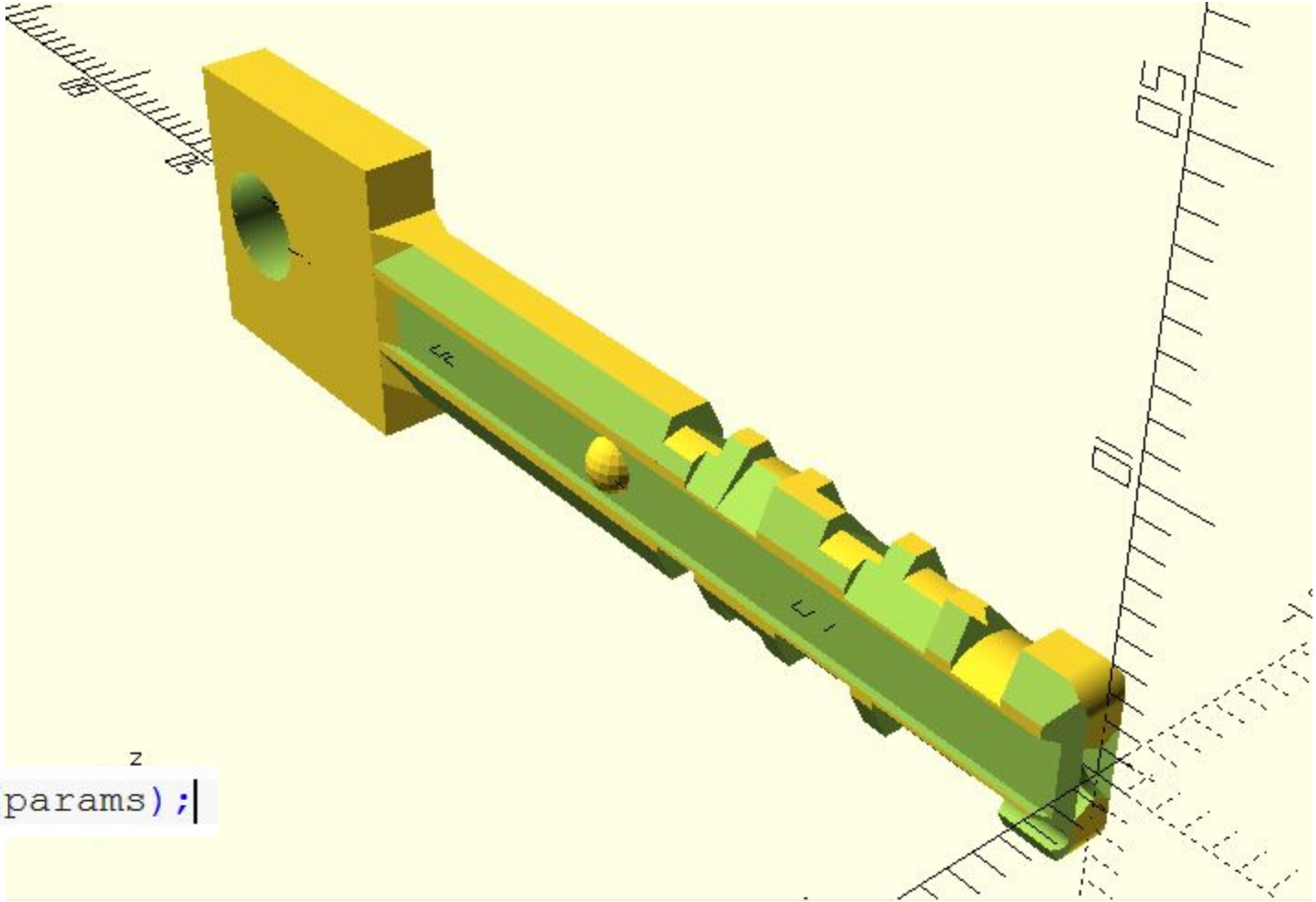
Bill Graydon,
Principal, Physical Security Analytics
GGR Security Consultants
1-800-833-0201 ext. 200
b.graydon@ggrsecurity.com

Vendor Response

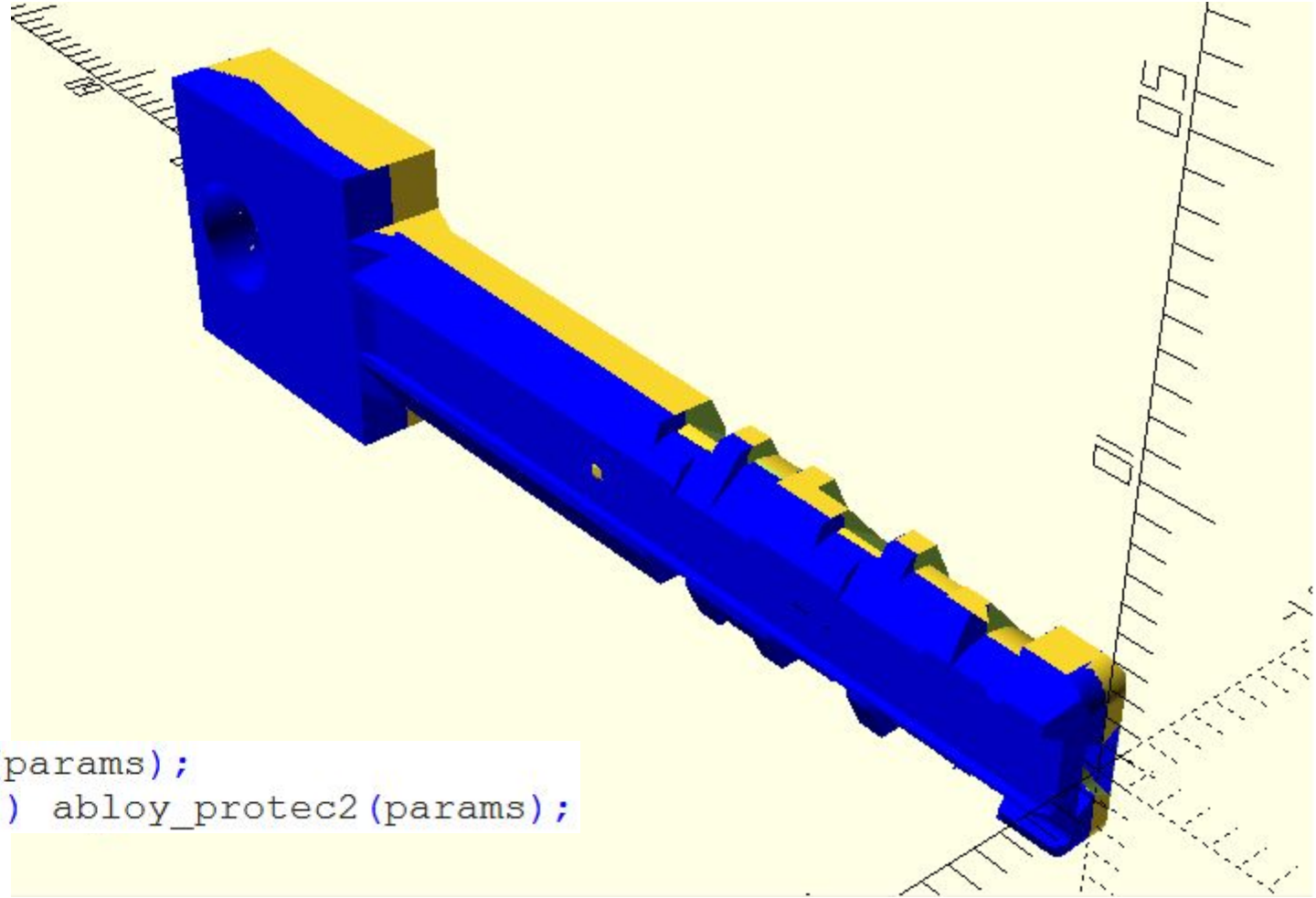



ABLOY
HARDENED

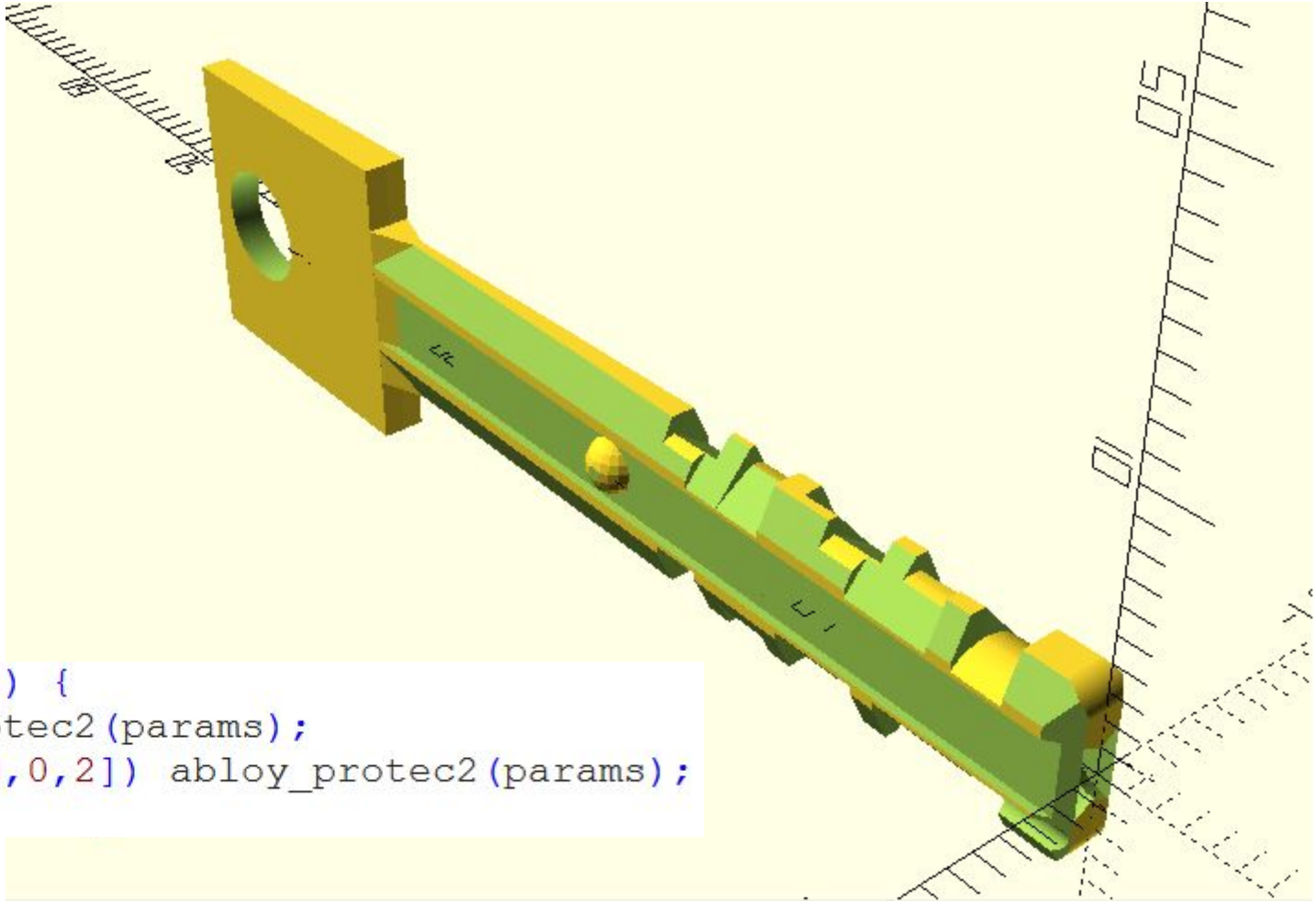

BORON
350
HARDENED
ABLOY
FINLAND



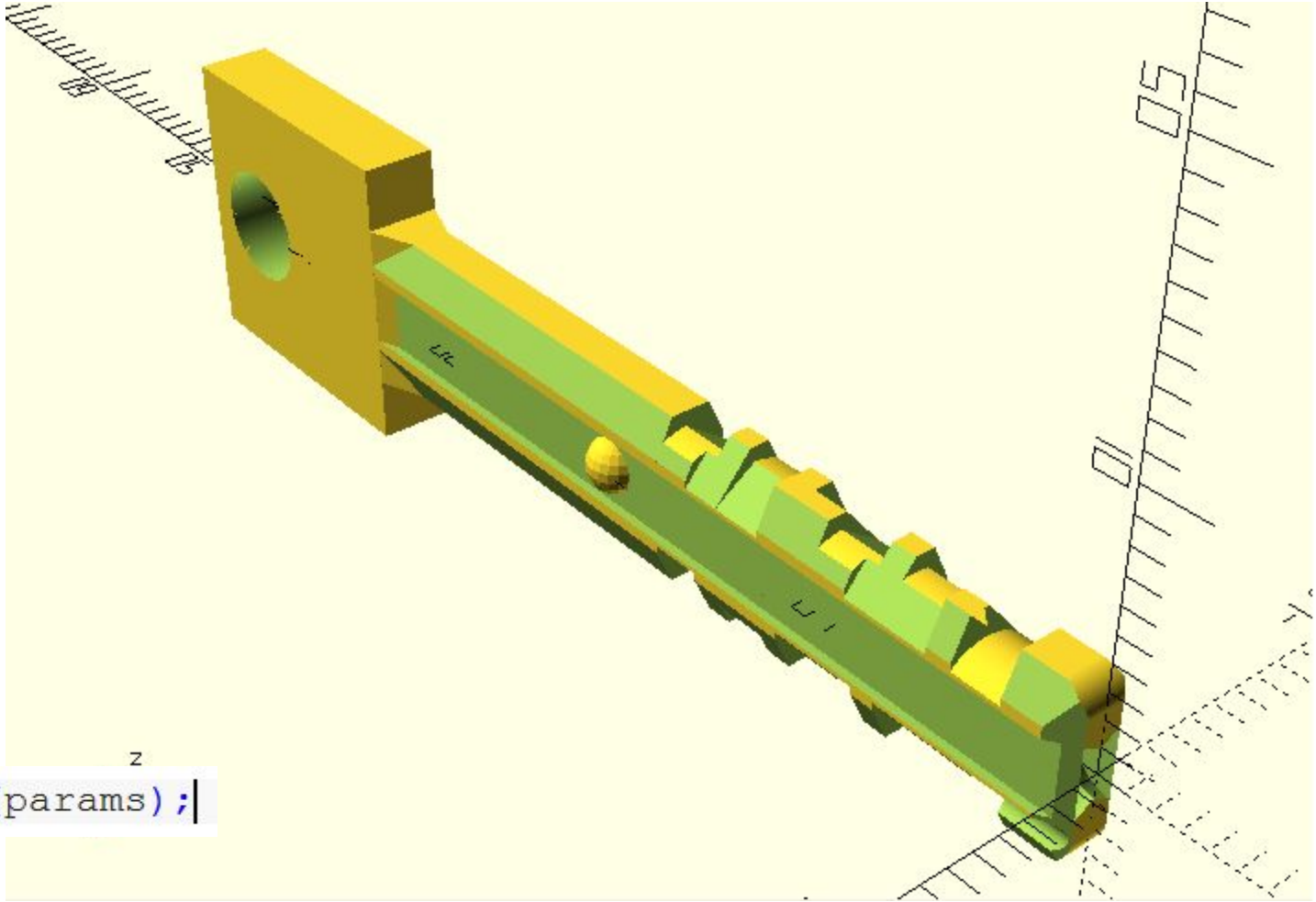

```
abloy_protec2(params);
```



```
abloy_protec2(params);
rotate([0,0,2]) abloy_protec2(params);
```

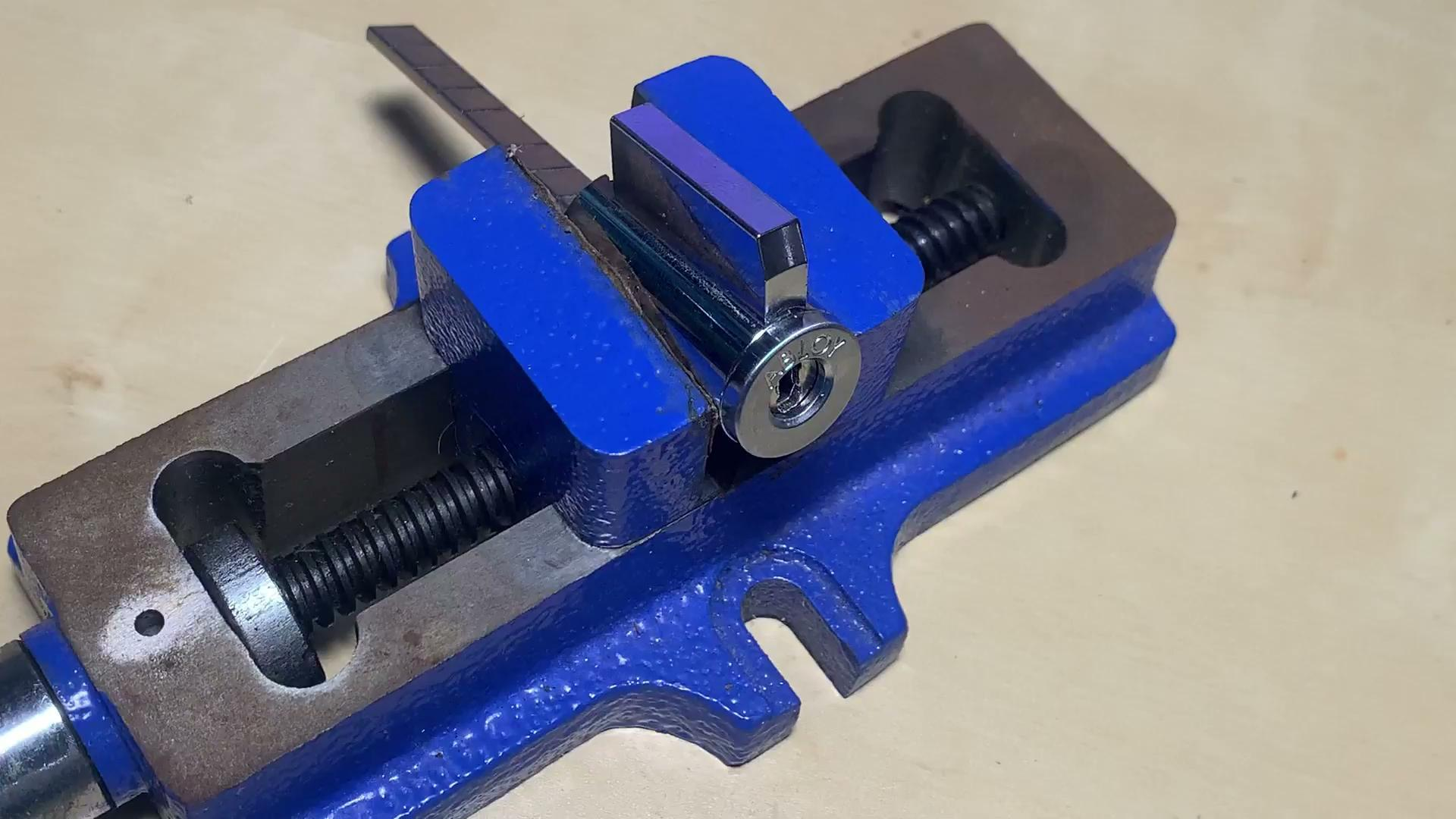


```
intersection() {
    abloy_protec2(params);
    rotate([0,0,2]) abloy_protec2(params);
}
```




```
abloy_protec2(params);
```


ABLOY
PAT.



To info@abloy.ca Date 2020-12-29 10:06

Hi folks,

I'd like to reach out to disclose two vulnerabilities we've discovered in the key control of Abloy Protec systems -

1) A means to defeat the interactive component of Protec2 locks by creating a key which operates the lock out of a single solid piece of material (including by 3D printing).
2) A means to copy the radial cuts of Protec and Protec2 using a standard key duplicator.

In order to keep end users and facility managers appraised of potential threat vectors to their key control, we plan to present this research publicly, tentatively in the summer of 2021. We're reaching out now to give you an opportunity to mitigate these vulnerabilities before we release them to the public.

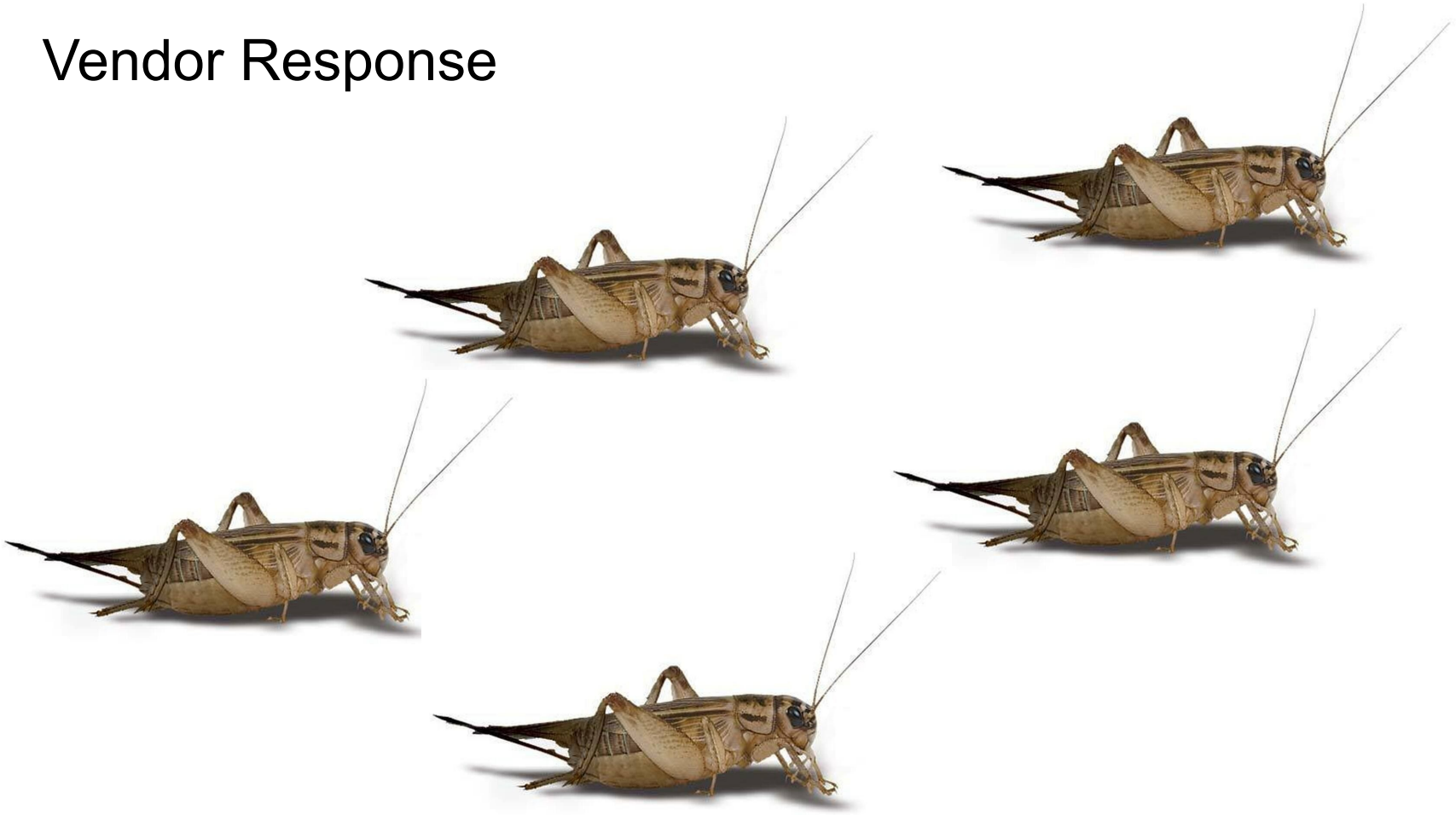
Please forward this to the appropriate department so we can send info and discuss further. We'd like to assist you in any way we can to mitigate these risks.

All the best,
Bill

--

Bill Graydon,
Principal, Physical Security Analytics
GGR Security Consultants
1-800-833-0201 ext. 200
b.graydon@ggrsecurity.com

Vendor Response




medeco
ASSA ABLOY
M4
5 IS


medeco


PAT. PENDING
M4
RESTRICTED
DO NOT DUPLICATE
medeco
PAT. NO. 4,835,455
medeco
SECURITY LOCKS
PAT. NO. 5,477,375
M3
SECURITY LOCKS
medeco
AREA NETWORK
HIGH SECURITY LOCKS

Security Technology

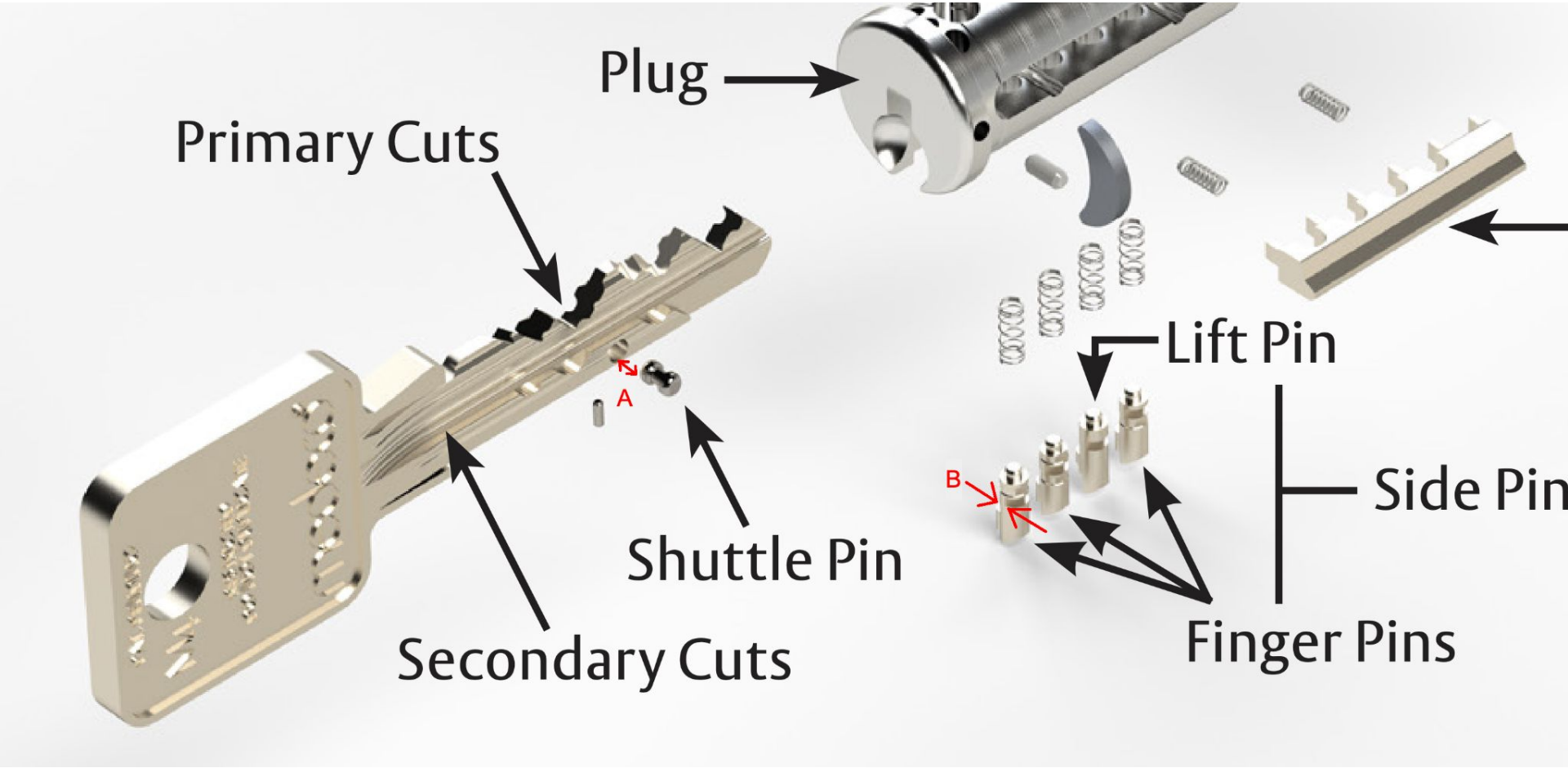
ASSA ABLOY Introduces Medeco 4 Locking System

M4's patent-pending key control protects against unauthorized duplication of keys, including unauthorized 3D printed copies.

January 17, 2021 CS Staff Jump to Comments

ASSA ABLOY, a manufacturer of access control solutions, introduces Medeco 4 (M4), a high-security key technology that is said to offer protection against physical attack and unauthorized key duplication.

M4 cylinders are UL Standard 437 listed for physical strength and high security, with solid brass machined construction and hardened-steel inserts to thwart drilling attacks. M4 cylinders are available in a wide variety of formats and are ideal for any application requiring key control and a high level of physical security.


Plug
Primary Cuts
A
Lift Pin
B
Side Pin
Shuttle Pin
Secondary Cuts
Finger Pins

Vendor Outreach

To info@medeco.com Date 2020-12-29 10:01

Hi folks,

I'd like to reach out to disclose two vulnerabilities we've discovered in the key control of Medeco systems -

1) A means to defeat the interactive component of the upcoming M4 locks by creating a key which operates the lock out of a single solid piece of material (including by 3D printing).
2) A means to copy the angled top cuts of all Medeco versions using a standard key duplicator.

In order to keep end users and facility managers appraised of potential threat vectors to their key control, we plan to present this research publicly, tentatively in the summer of 2021. We're reaching out now to give you an opportunity to mitigate these vulnerabilities before we release them to the public.

Please forward this to the appropriate department so we can send drawings and info, and discuss further. We'd like to assist you in any way we can to mitigate these risks.

All the best,

--

Bill Graydon,
Principal, Physical Security Analytics
GGR Security Consultants
1-800-833-0201 ext. 200
b.graydon@ggrsecurity.com

Vendor Response

Later that day…

Hi Bill,

Thanks for reaching out. When can we speak by phone?

Regards,
Clyde

Clyde T. Roberson, CML, AHC, CPP, CMST
Medeco Security Locks, INC
Director of Product Management and Field Services
3625 Alleghany Drive
Salem, VA 24153 USA
540.380.1654
540.380.1768 fax
www.medeco.com

From: Stewart, Brenda <brenda.stewart@assaabloy.com>
Sent: Tuesday, December 29, 2020 10:11 AM
To: Roberson, Clyde <Clyde.Roberson@assaabloy.com>
Cc: Esposito, Amy <Amy.Esposito@assaabloy.com>
Subject: FW: [EXT] Robert Goldberg <r.goldberg@ggrsecurity.com>, Robert Graydon <r.graydon@ggrsecurity.com>

Vendor Response

Clyde Roberson's Zoom Meeting

From Roberson, Clyde <Clyde.Roberson@assaabloy.com> Date 2020-12-30 13:03

Part 3.ics (~3 KB)

Invitation to Clyde Roberson's Zoom Meeting
Date 2020-12-30 15:30 - 16:00
Location https://assaabloy.zoom.us/j/92789881793?pwd=b0N0LzdHYnVzZUJod1Z4ckRhUkM4UT09

Do you accept this invitation?

Accept | Maybe | Decline | Delegate | Check Calendar

Do not send a response Enter a response text

Agenda 2020-12-30

No earlier events
15:30 - 16:00 Clyde Roberson's Zoom Meeting
No later events

Hi Bill, just so we don't keep missing each other, would you be ok with 3:30 today for a call or ZOOM? Looking forward to speaking with you….

Thanks, Clyde

zoom

Hi there,

Clyde Roberson is inviting you to a scheduled Zoom meeting.

Join Zoom Meeting

Phone one-tap: US: +13126266799,,92789881793#,,,,*518652# or

Good Response!

- Calls
- Discussion of Technique
- Medeco’s team tried it
  - without success
- My turn to try it
- But first…

MUTUAL NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THIS MUTUAL NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT ("Agreement") is made between ASSA ABLOY Inc. and/or any of its directly or indirectly wholly-owned subsidiaries or affiliated group companies who are identified below (together or individually, "ASSA ABLOY") and the participant identified below ("Participant") (ASSA ABLOY and the Participant are hereinafter collectively referred to as the "Parties" or individually referred to as a "Party") in connection with the activities or work described in the attached Exhibit A (the "Work").

1. **Confidential Information**. As used herein, Confidential Information includes any information or data (in any form or medium) disclosed by one Party (the "Discloser") to the other Party (the "Recipient") and includes, but is not limited to, all information concerning Discloser's products, such as product and manufacturing drawings, product samples, bills of materials, technical data, sourcing information and any other information which (a) if in tangible form or other media that can be converted to readable form is clearly marked as proprietary, confidential or private when disclosed, or (b) if oral or visual, is identified as proprietary, confidential, or private when disclosed, or (c) by its very nature constitutes information of a type that any reasonable business person would conclude was intended by Discloser to be treated as proprietary, confidential, or private, regardless of whether such information was marked or identified as proprietary, confidential, or private. Confidential Information may include any business, technical, financial or strategic planning information which has been or may hereafter be provided by Discloser to Recipient, including without limitation, financial condition, market share, trade secrets, inventions, copyrights, know-how, marketing, software, computer and security systems or other compilations of information which are used in Discloser's business or products and which give Discloser an opportunity to obtain an advantage over its competitors who do not know and/or do not use it (which includes, but is not limited to, databases and database management systems, software and software management, source code, customer and subscriber lists and other information relating to the same, pricing or financial information, intangible property and other such information or intellectual property which is not in the public domain). Notwithstanding the foregoing, Confidential Information for purposes of this Agreement will include all information disclosed by Discloser to Recipient in connection with the Work, including but not limited to product information and strategy relating to manufacturing and costs, pricing, marketing,

to avoid disclosure to any third party as is used with respect to Recipient's own information of like importance which is to be kept secret, but in no event with less than a commercially reasonable degree of care; (d) not disclose the Confidential Information to any person other than its Advisors who reasonably require access in order to fulfill Recipient's obligations in connection with the Work, and in connection with any such disclosure ensure that each such Advisor is aware of the confidential nature of the Confidential Information and that it is governed by this Agreement and either: (i) has signed an equivalent confidentiality agreement that applies to the Confidential Information disclosed hereunder; or (ii) has executed a copy of the "Non-Disclosure Acknowledgment and Certification" attached hereto as Exhibit B; (e) Without in any way limiting the generality of the foregoing, Recipient agrees that in connection with any disclosure to any sub-contractor or any other person who is an Advisor (except for any directors, officers or employees), Recipient must obtain prior written permission from Discloser and require any such individual to whom it intends to divulge the Confidential Information to sign a copy of the Non-Disclosure Acknowledgment and Certification referenced above prior to Recipient's disclosure of the Confidential Information; (f) inform Discloser immediately upon becoming aware of, or having reasonable grounds to suspect, that any person other than an Advisor has obtained access to the Confidential Information; (g) be wholly and fully liable towards Discloser for all actions of its Advisors in connection with the Confidential Information; and (h) indemnify and hold harmless Discloser for any claims made by a third party as a result of Recipient's or any of its Advisors' improper use of the Confidential Information.

4. **Exclusions**. The obligations of Paragraph 3 shall not apply to any Confidential Information which Recipient can demonstrate: (a) is or becomes available to the public through no wrongful act,

Subject to any written agreement between the Parties to the contrary: (a) all Foreground Intellectual Property will belong to and vest in ASSA ABLOY, free from any claim or retention of rights by Participant or any related company or third party retained by the Participant in connection with the Work. The Participant shall keep a record of and promptly disclose to ASSA ABLOY any Foreground Intellectual Property developed by it or on its behalf in connection with the Work. The Participant will do all such things and execute all documents necessary to enable ASSA ABLOY to obtain, defend or enforce its rights in such Foreground Intellectual Property and to assist ASSA ABLOY, upon ASSA ABLOY's request and in its sole discretion, in applying in the United States and any other country for letters patent with respect to any invention or improvement comprised within the Foreground

On 2021-03-17 16:23, [redacted] wrote:

Good afternoon Mr. Graydon,

Please find attached the mutual NDA with the 2nd paragraph deleted. If you need anything further, please let me know.

Thank you!

[redacted]

Legal Administrator

Medeco, a division of ASSA ABLOY High Security Group Inc

ASSA ABLOY Opening Solutions

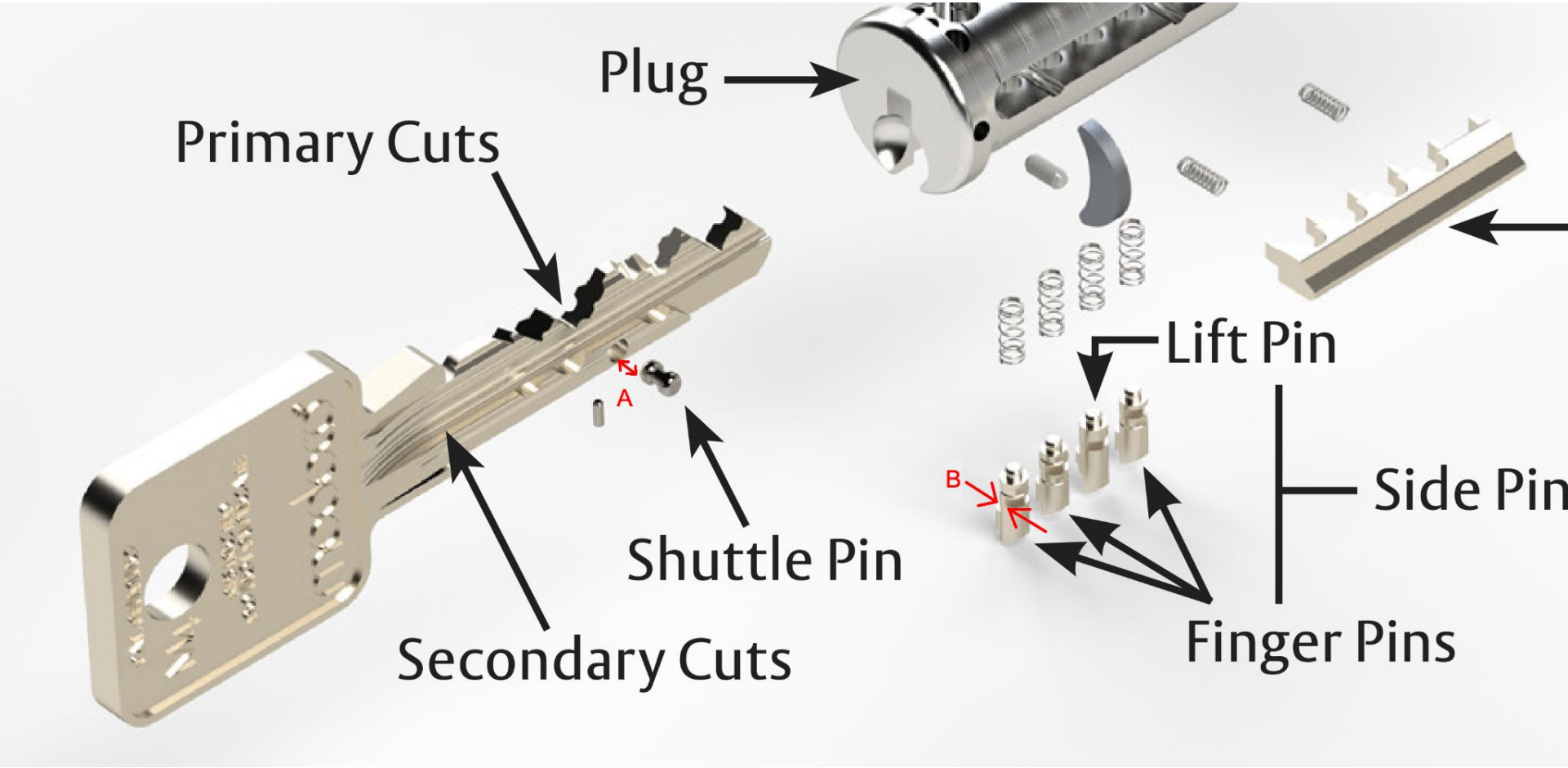
3625 Alleghany Drive

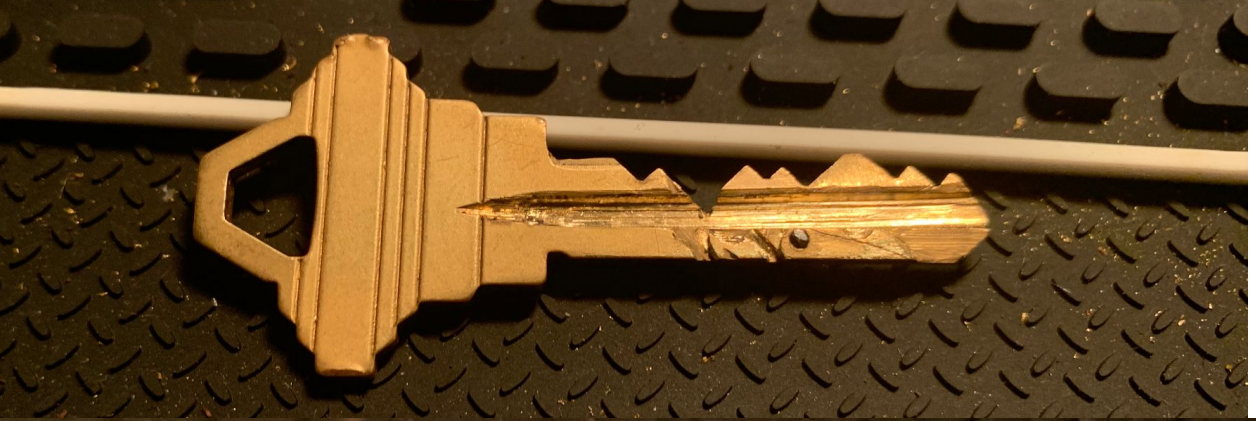
Salem, VA 24153

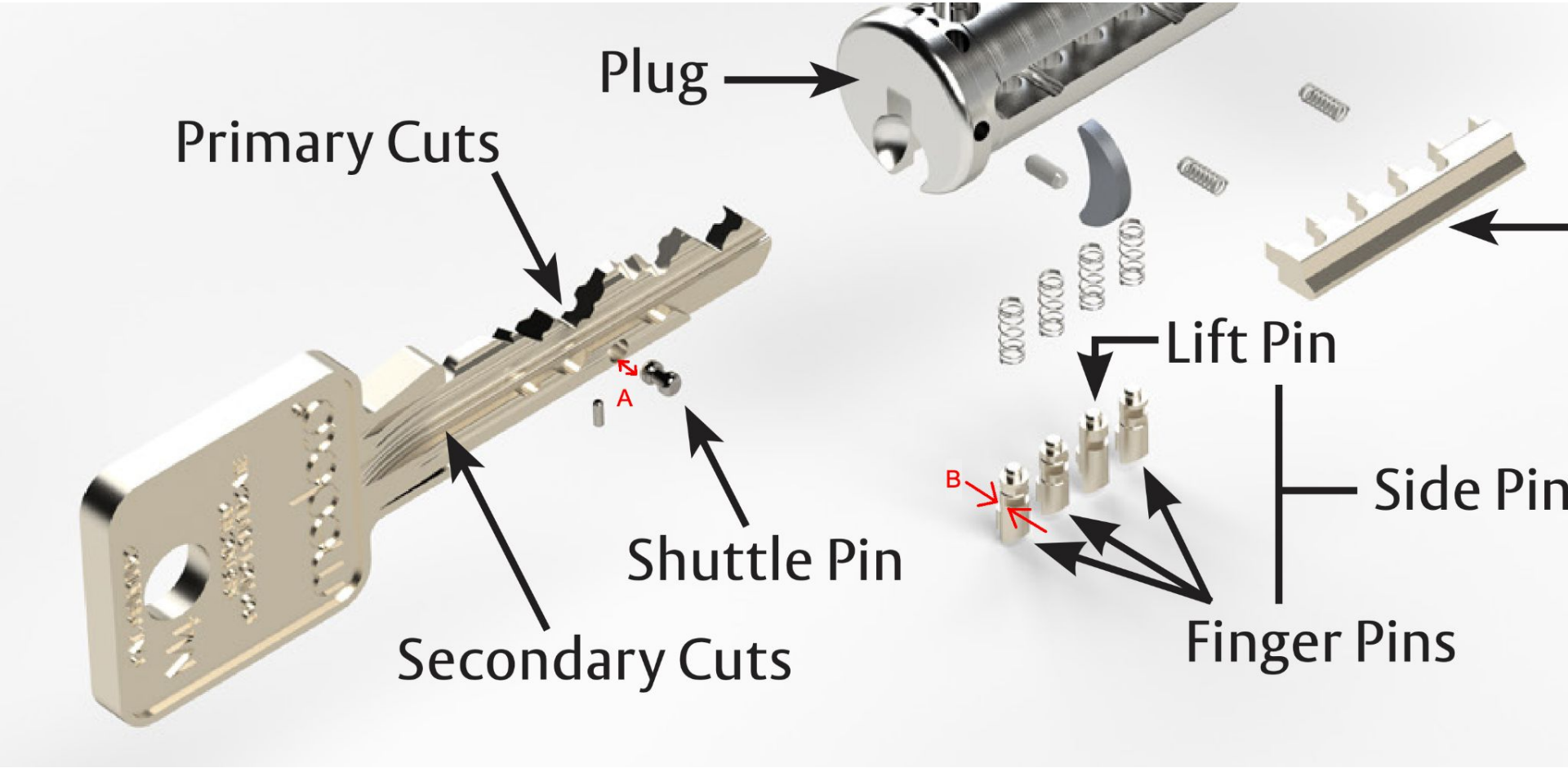
All Signed

Attempt #1


MEXICO
SC9

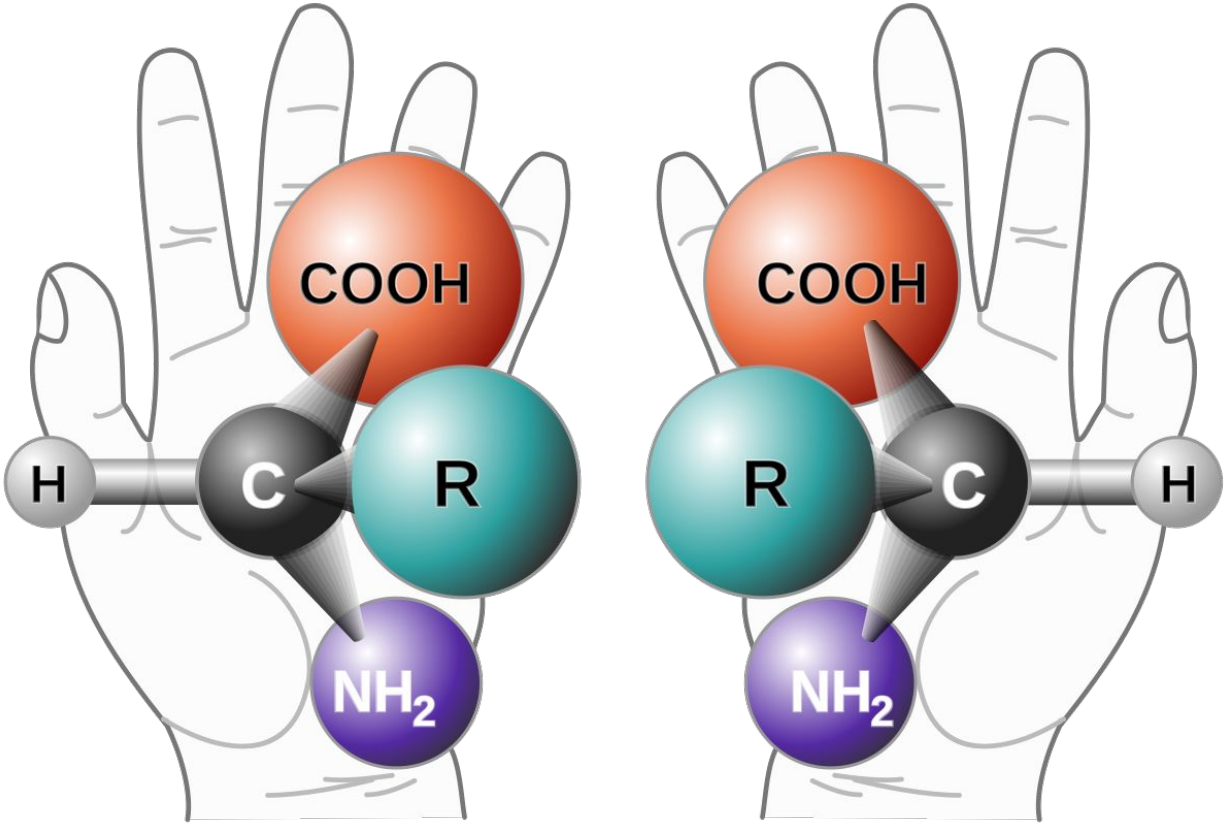

Plug
Primary Cuts
A
Lift Pin
B
Side Pin
Shuttle Pin
Secondary Cuts
Finger Pins



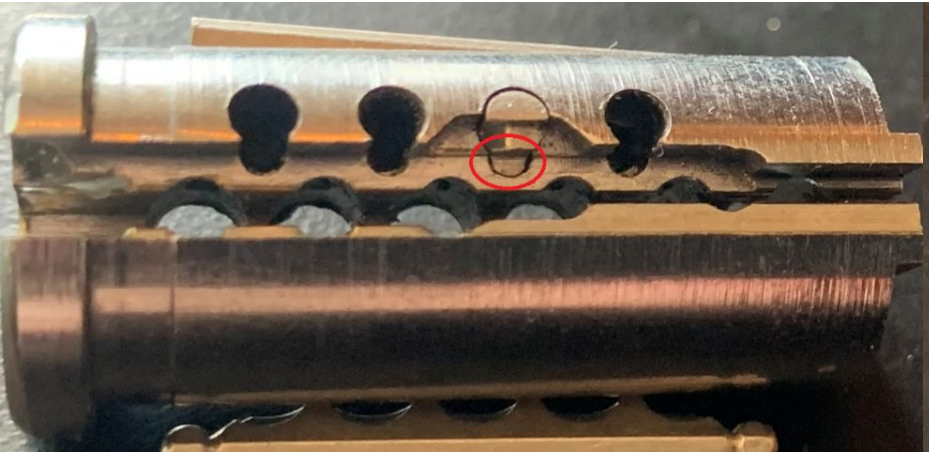

Plug
Primary Cuts
A
Lift Pin
B
Side Pin
Shuttle Pin
Secondary Cuts
Finger Pins

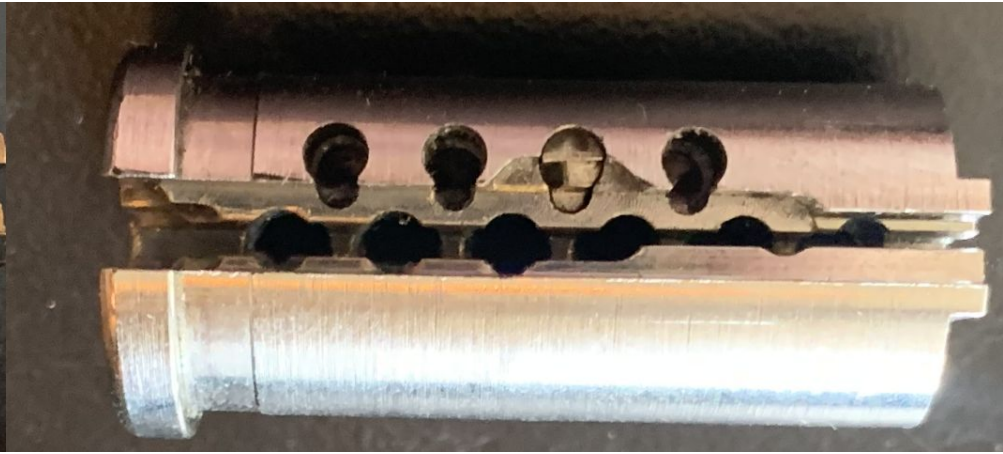
Attempt #2

Chirality Matters (kind of)

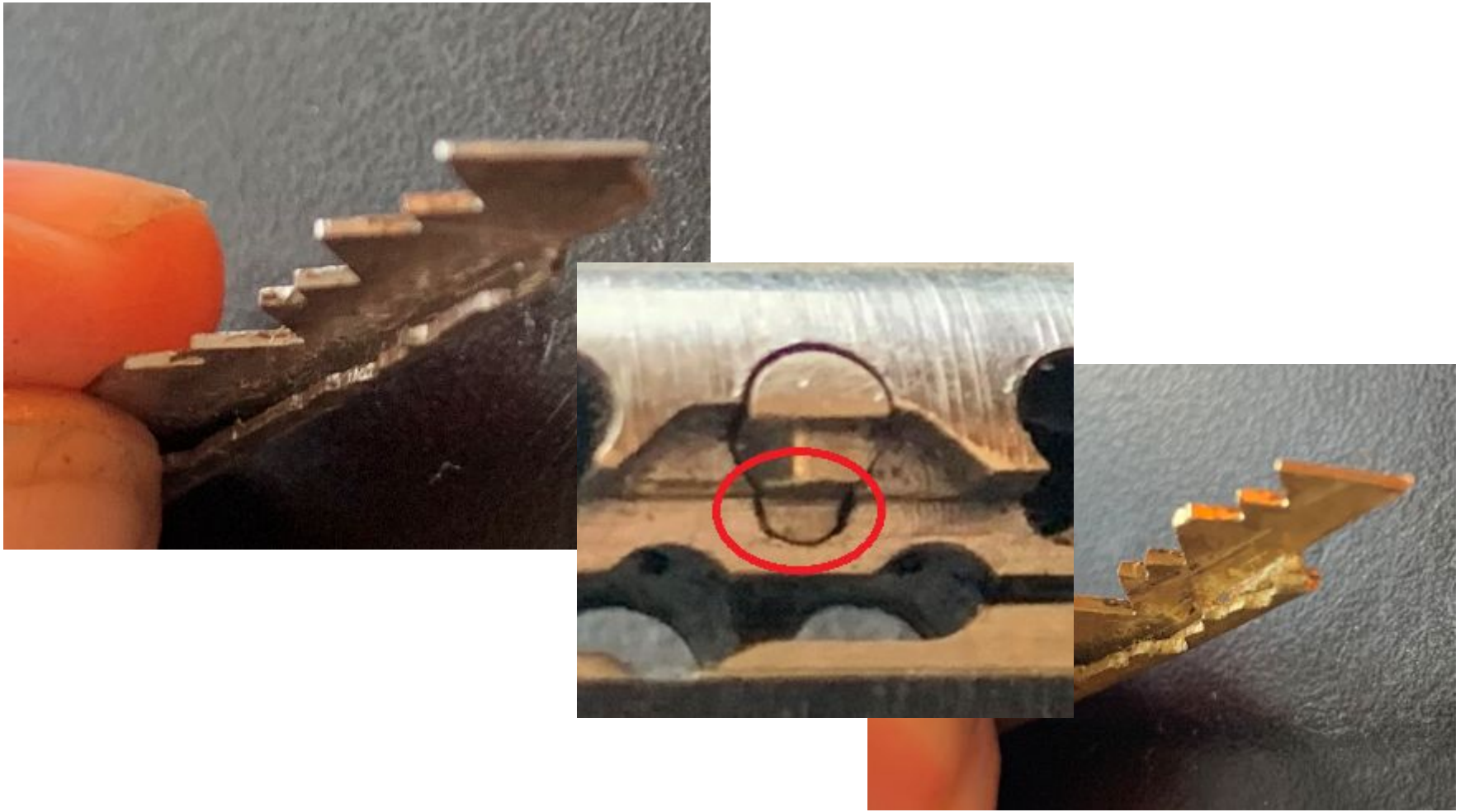


Attempt #3






medeco
RESTRICTED
DO NOT DUPLICATE

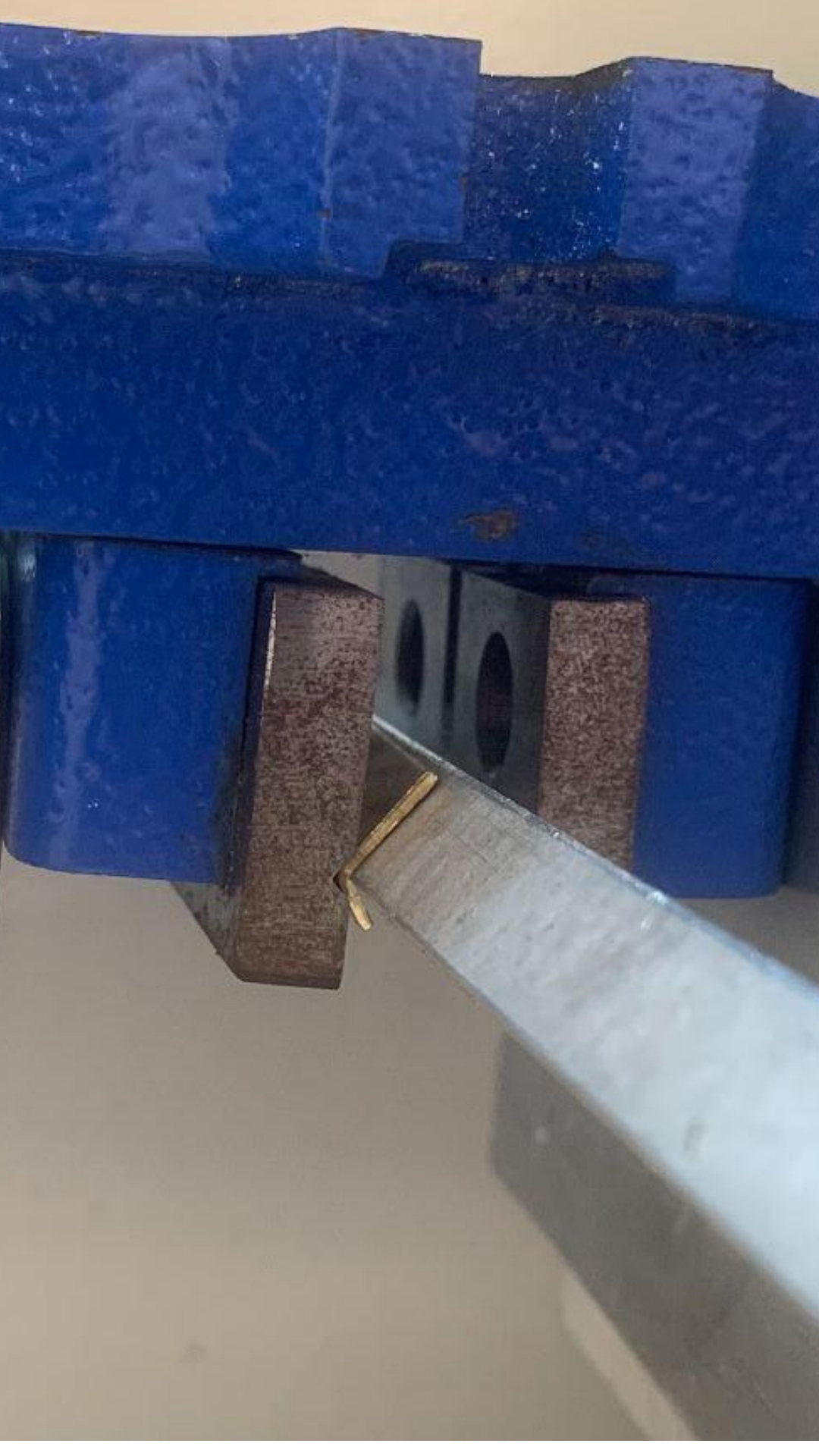


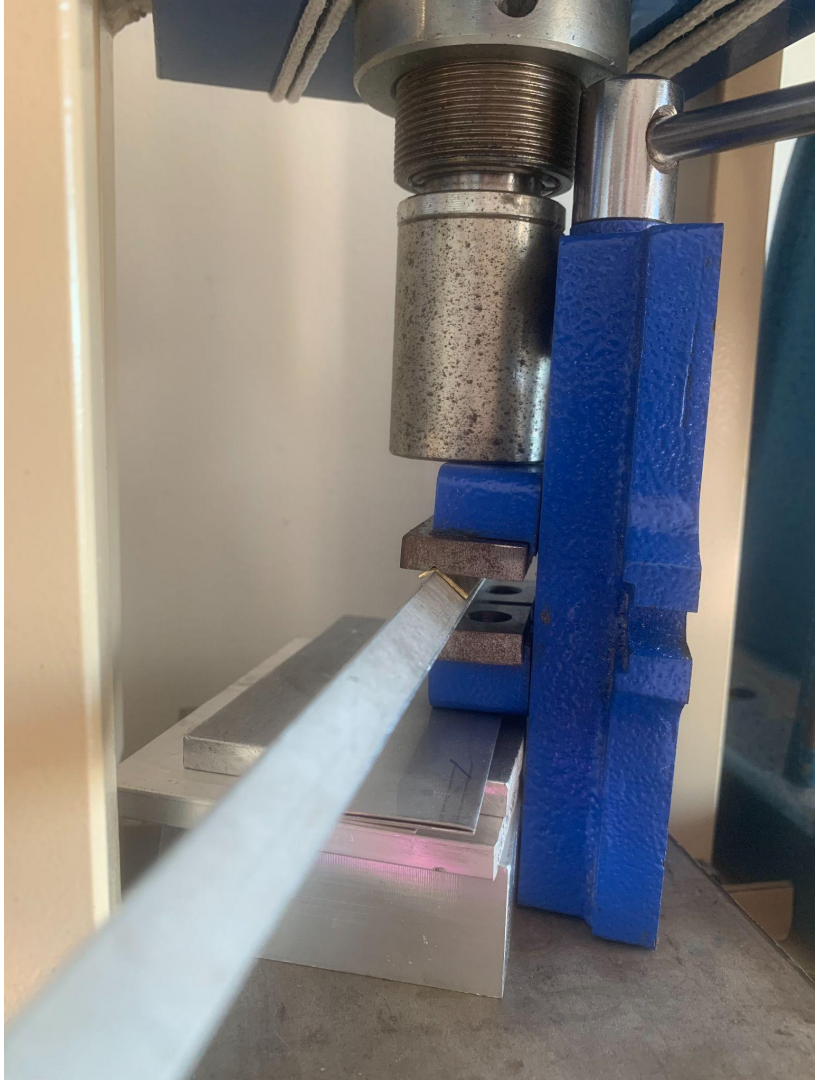

medeco
ASSA ABLOY

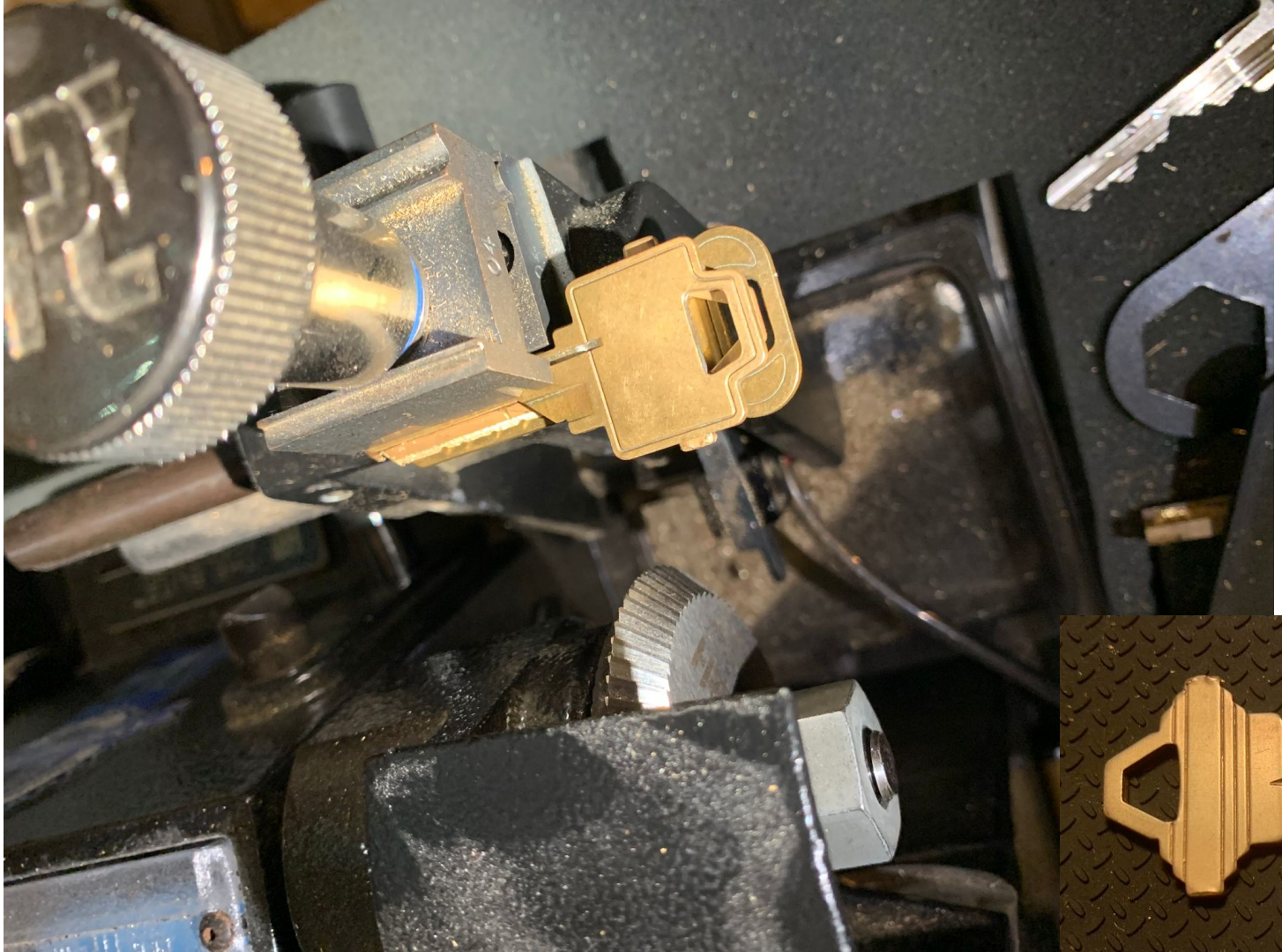
Fabrication

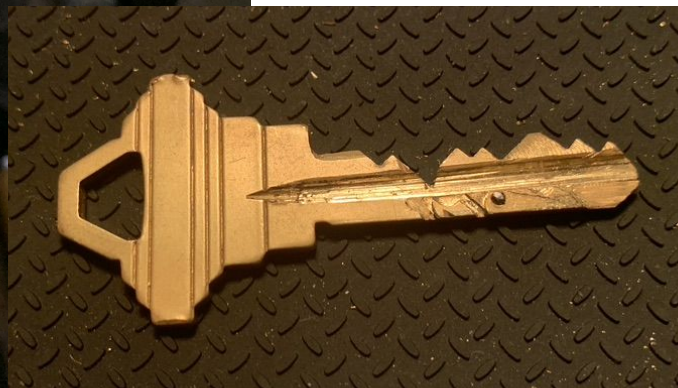

Ender


CREALITY
CREALITY









02211
26895
26211
26215
26811
26815
hh1
111

Patents are effective(ish) against mass production

U.S. Patent Aug. 15, 1989 Sheet 1 of 2 4,856,309

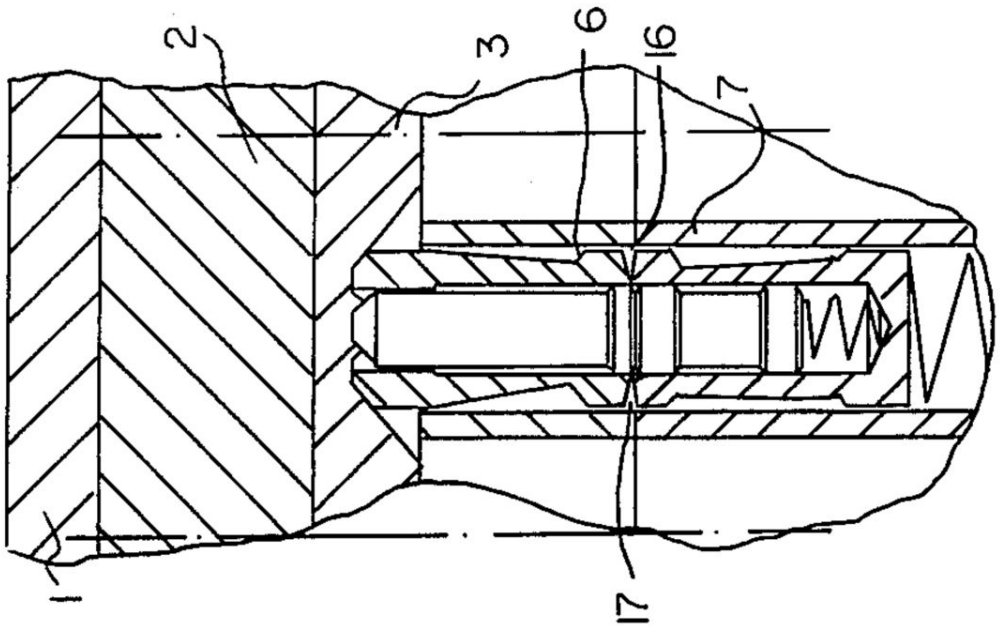


FIG. 2
PRIOR ART

Key tool B316 Home Door Key blanks Locksmith Supplies Blank Keys 20 pieces/lot

★★★★★ 5.0 3 Reviews 5 orders

US $12.25 / lot (20 Pieces)

~~US $12.90~~ -5%

US $3.00 off Coupons For You Get coupons

Quantity: 1 959 lots available

Ships to United States

Shipping: $1.60

From China to United States via AliExpress Standard Shipping

Estimated delivery on Aug 17 More options

Buy Now Add to Cart ♡ 22

75-Day Buyer Protection
Money back guarantee

Free Return
Return for any reason within 15 days

Recommended For You

US $12.06

US $2.03

US $13.77

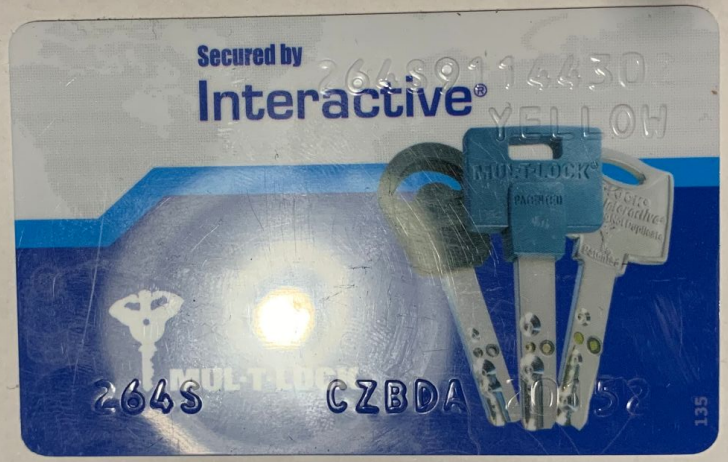
Alternative Attacks

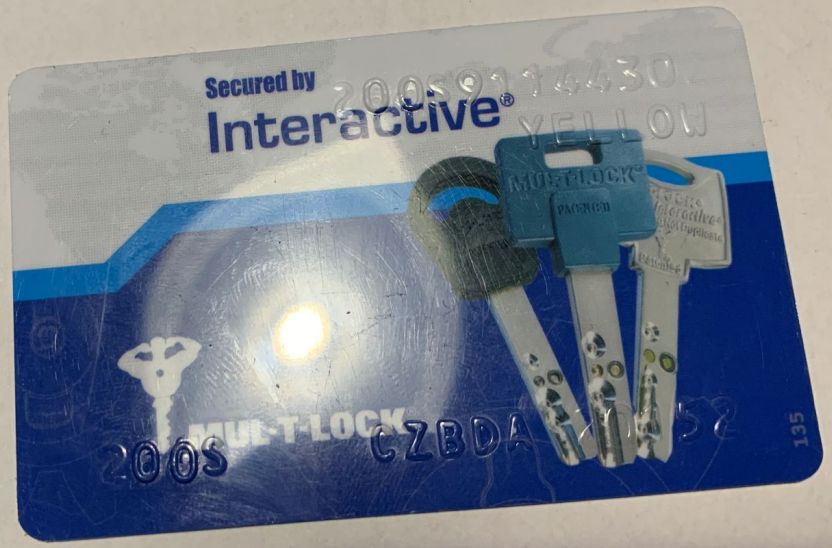

8288
8287
New York City Subway

EBay stops selling keys that could open New York City to terrorists

By Susan Edelman

September 26, 2015 | 11:50pm


Secured by
Interactive®
MUL-T-LOCK
264S
CZBDA
135


Secured by
Interactive®
MUL-T-LOCK
200S
CZBDA
135

ORDER DATE
Nov 24, 2020

ORDER NUMBER
174245182176-2235791658007

SOLD BY
sky-baywarehouse

Box of 50, MUL-T-LOCK 264B+ NS Key Blanks, 51268800, Skbawa-b129-jb

(174245182176)

ITEM PRICE:
US $235.20

ORDER DATE
Nov 24, 2020

ORDER NUMBER
303545443592-18111117 65020

SOLD BY
justperfectdeals2011

50 PCS 264S KEYWAY MUL-T-LOCK INTERACTIVE PROFILE KEY BLANKS LOCKSMITH SUPPLY

(303545443592)

ITEM PRICE:
US $199.00

Name:
E-Mail: b.graydon@ggrsecurity.com
Company: GGR Security
Phone: 1-800-833-0201 ext 200
City: Toronto
Province: Ontario
Best time to contact:
Comment: Hi folks,

I purchased a box of 50 Mul-T-Lock interactive 264B blanks from EBay, which arrived with coining on the head for your company and phone number.

I was surprised to see the 416 area code, given that the listing was from Niagara Falls, and further surprised when I looked you up and found that you are still in business and servicing Mul-T-Locks (presumably under an inventory control contract).

All of this didn't add up, which piqued my suspicion that the blanks I purchased might be stolen property. I thought I should reach out to you in case you've recently experienced a theft of any sort, or in case any of your employees are otherwise engaged in unauthorised activities.

Please advise as to the situation, and let me know if I can be of assistance in any way.

All the best,
Bill.

On 2020-12-15 15:12, [redacted] wrote:

> Thanks for letting us know clearly they would be stolen blanks as we would never sell on ebay what is best number to speak with you

[redacted]

[redacted]
President

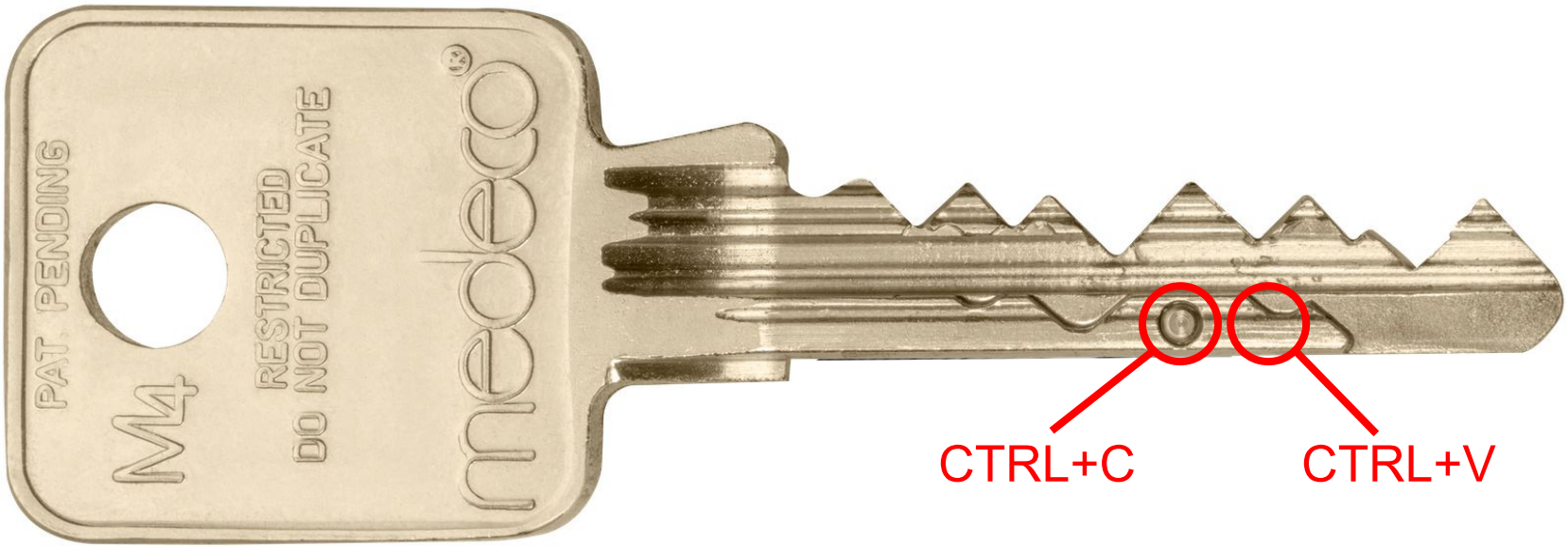
[redacted] **Security Services, Inc.**
Main Office: [redacted]

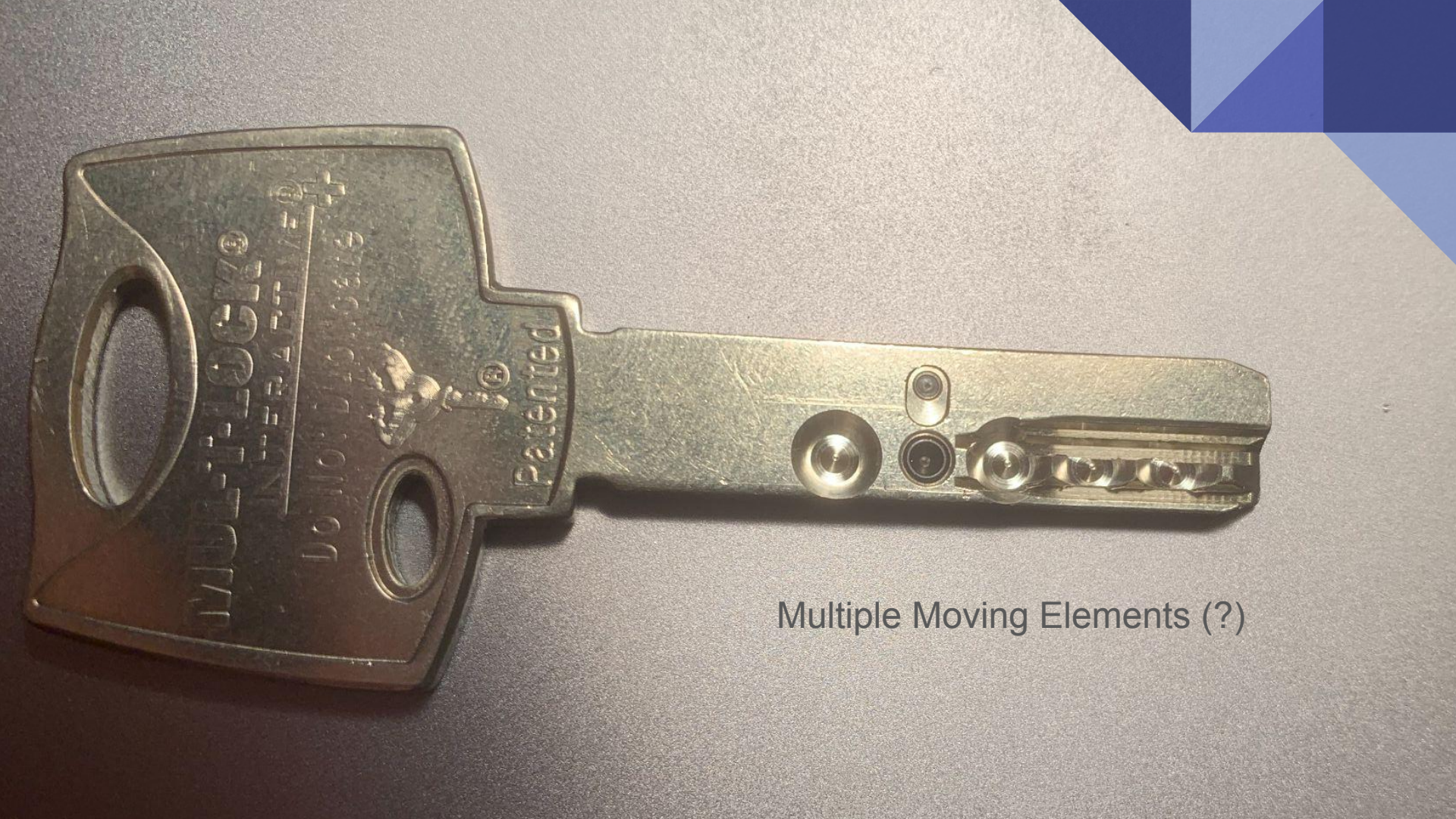
Fax:
Web: [redacted]

The Outcome…

- They traced it to a theft from courier package 3 years ago
- Ordered more blanks by courier
- Driver delivered - “this doesn’t feel like 25lbs”!
- Reported to Mul-T-Lock
- I reached out
- Recovered 9/10 stolen boxes (including mine)
- No compensation owed for stolen property
- They insisted on it anyway

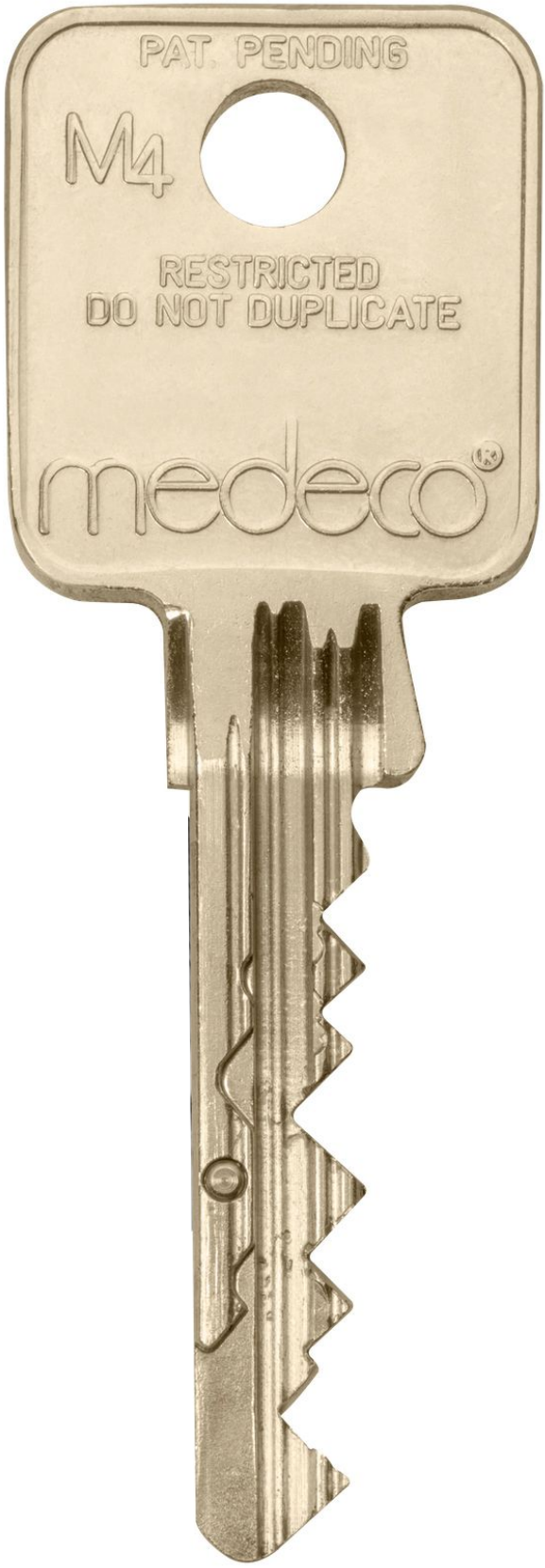
Defences

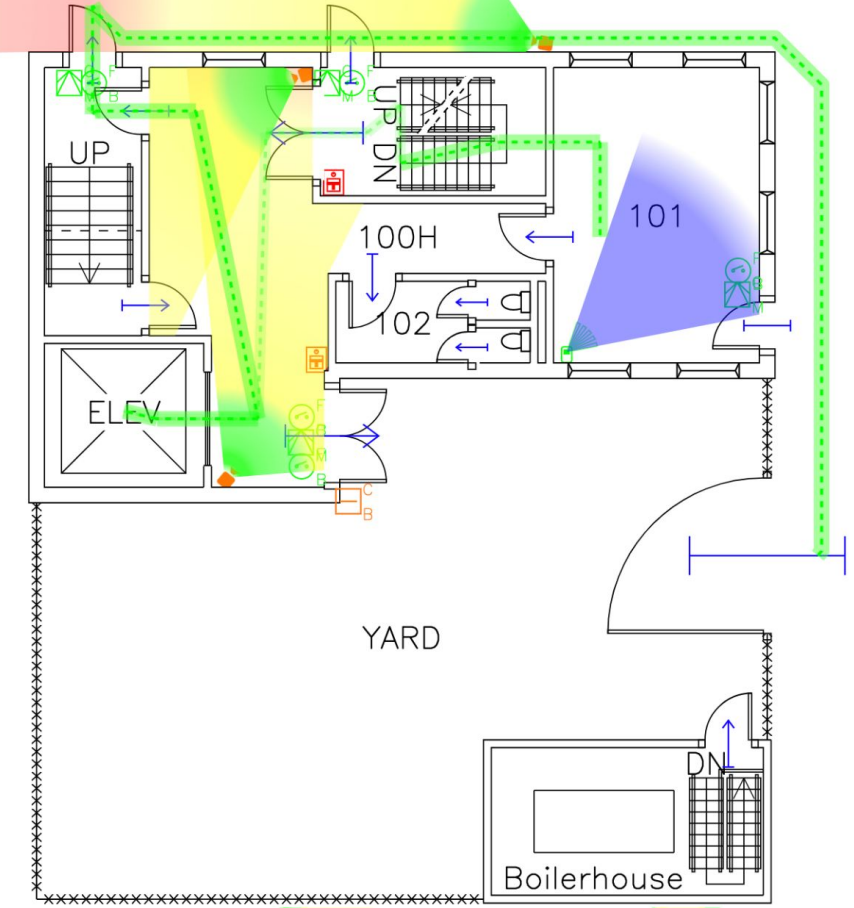

PAT. PENDING
M4
RESTRICTED
DO NOT DUPLICATE
medeco
CTRL+C
CTRL+V



Multiple Moving Elements (?)

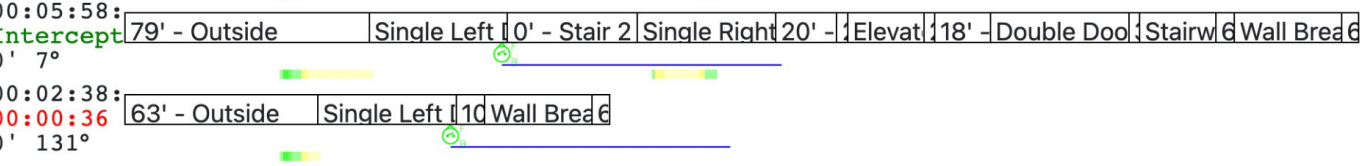

DO NOT DUPLICATE


PAT. PENDING
M4
RESTRICTED
DO NOT DUPLICATE
medeco®



Intercept the Attacker

1. Detect the Intrusion
2. Delay the Intruder after detection
3. Respond to the Intrusion in time
4. Intercept the intruder with greater force



Questions?

b.graydon@ggrsecurity.com

@access_ctrl

Or come find me in the Physical Security Village!