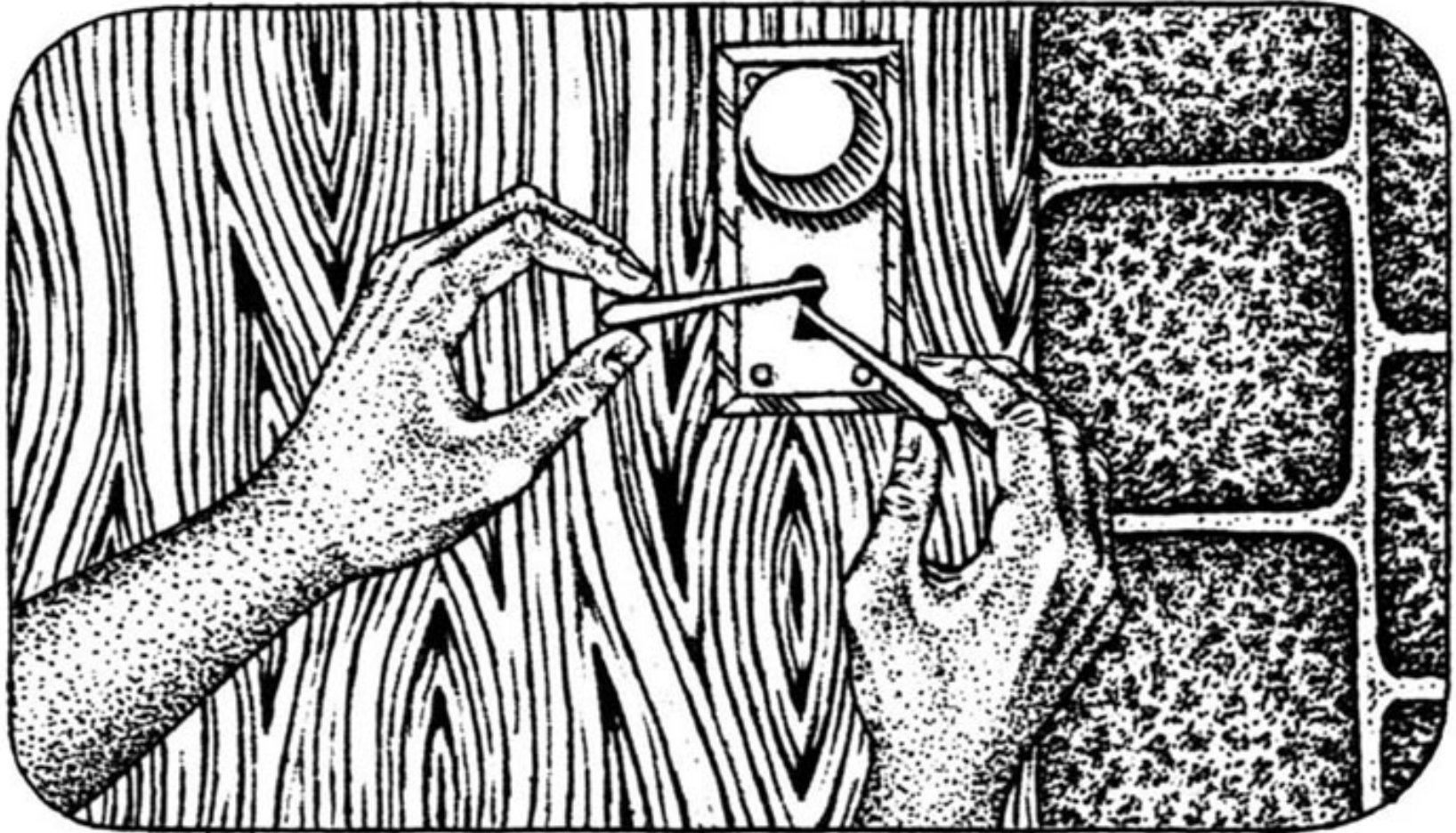


Ten Things Everyone Should Know About Lockpicking & Physical Security



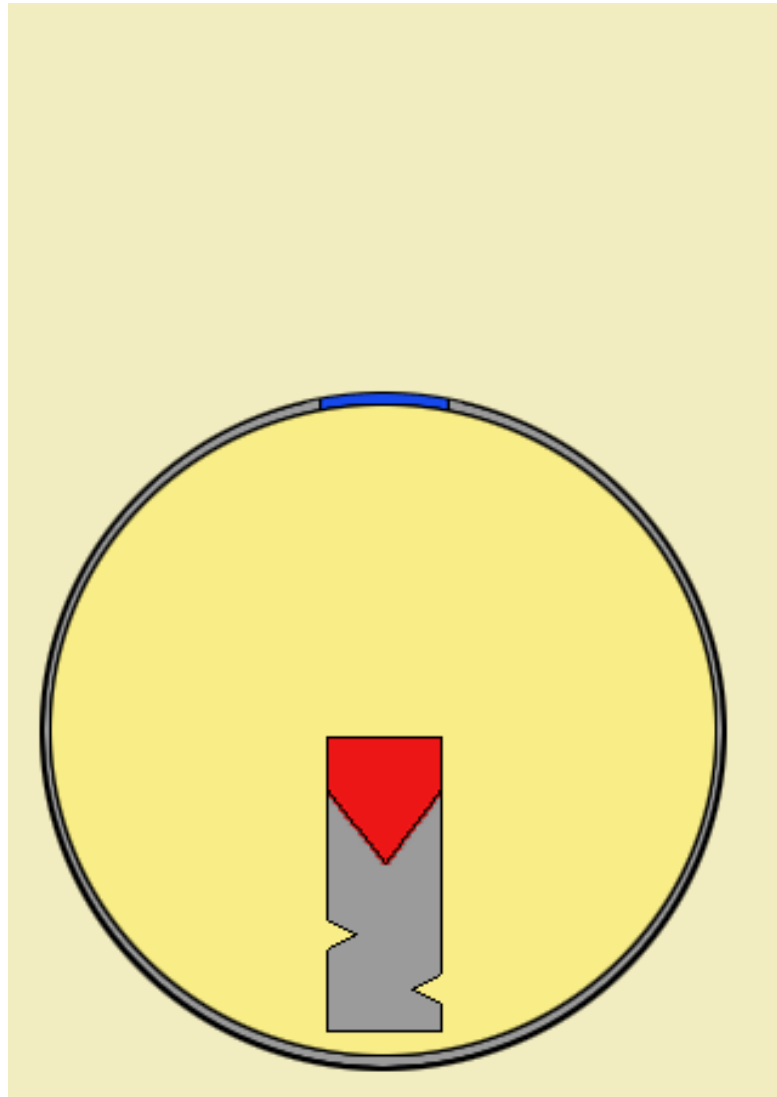
Deviant Ollam

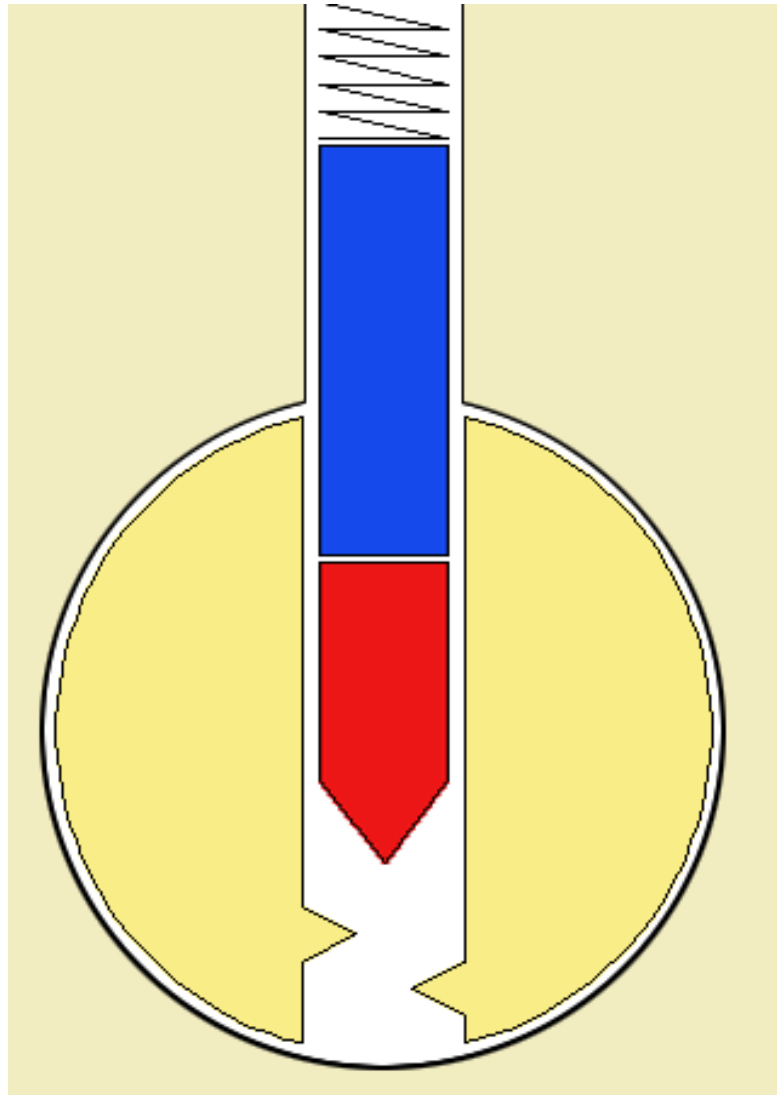
Black Hat Europe – 2008/03/25

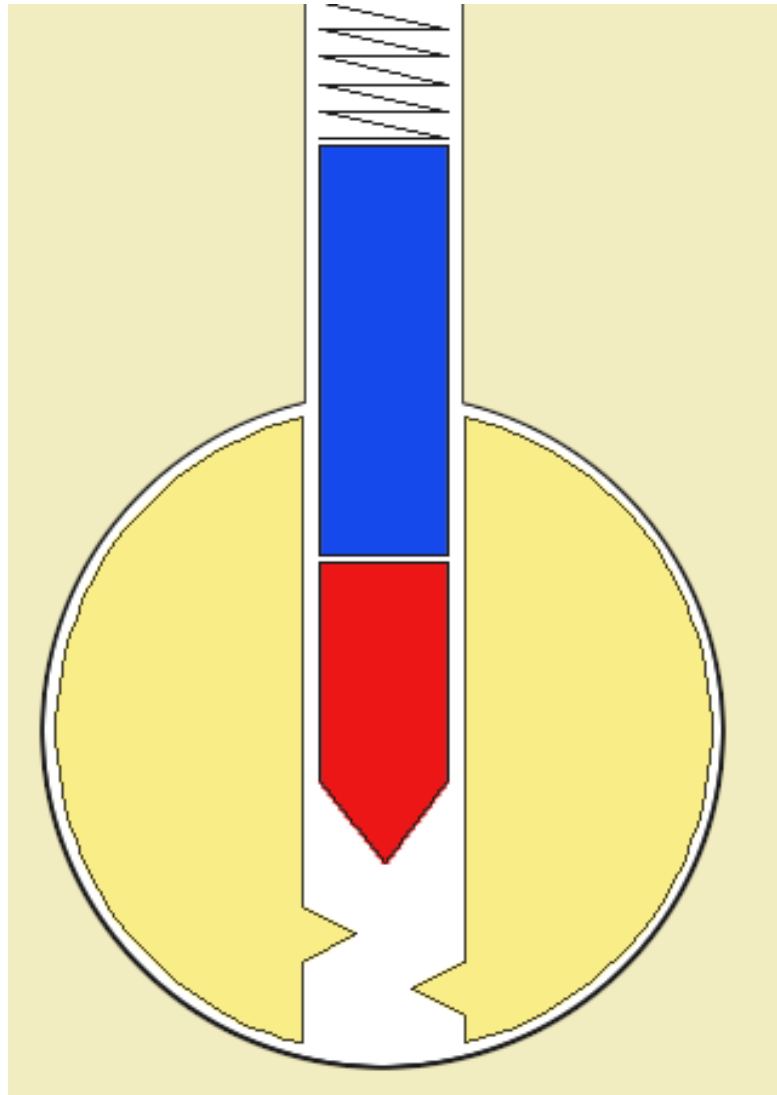
1. Locks are not complicated mechanisms

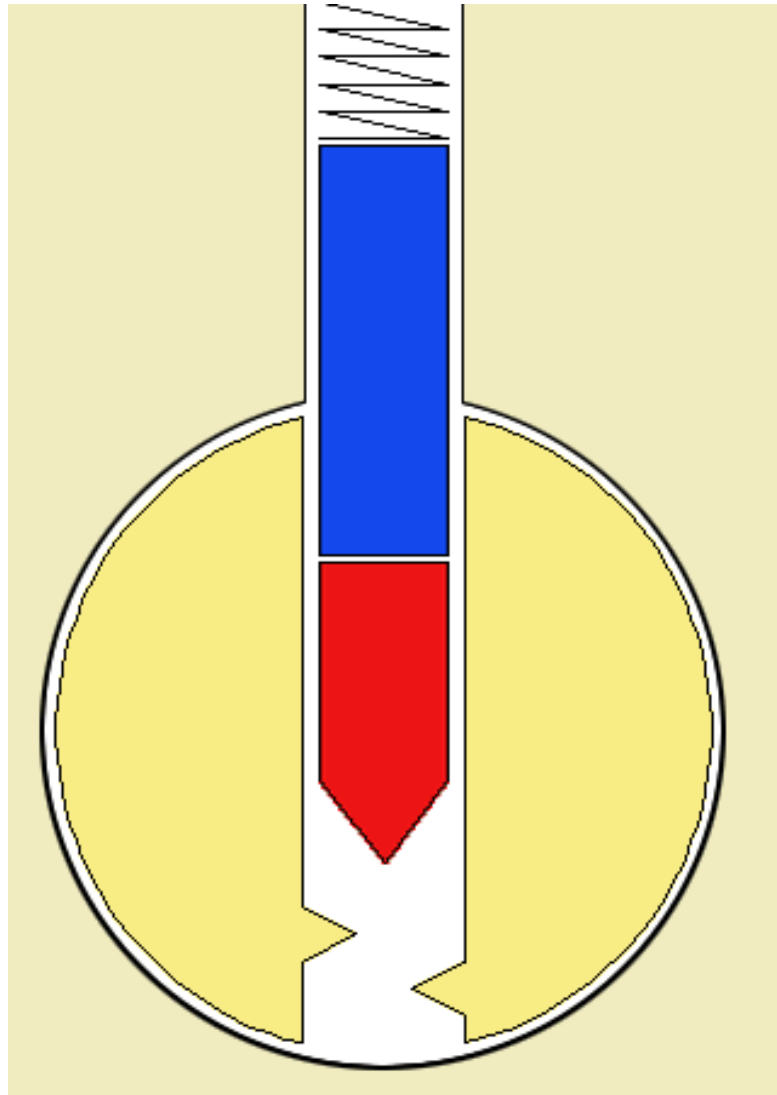
- Simple components
- Simple operation
- Efficient & resilient

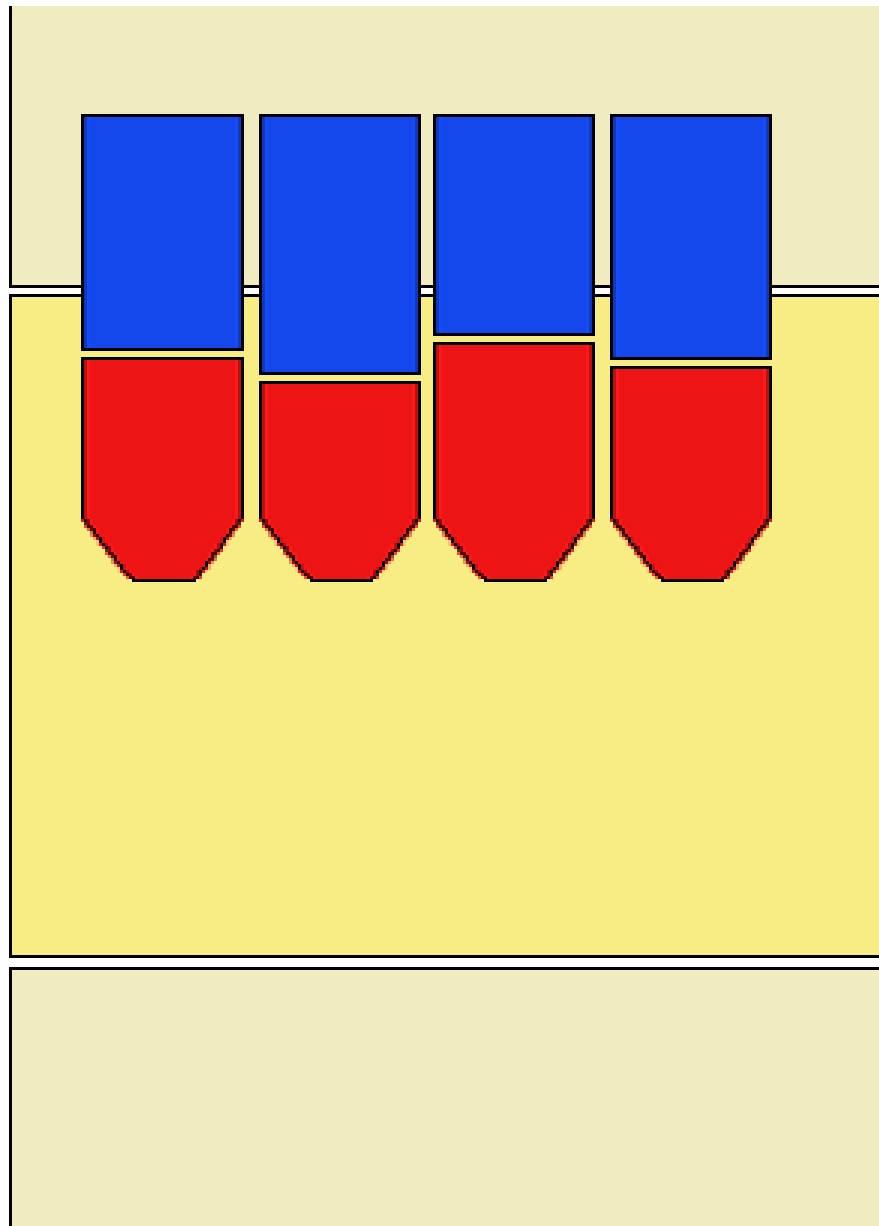








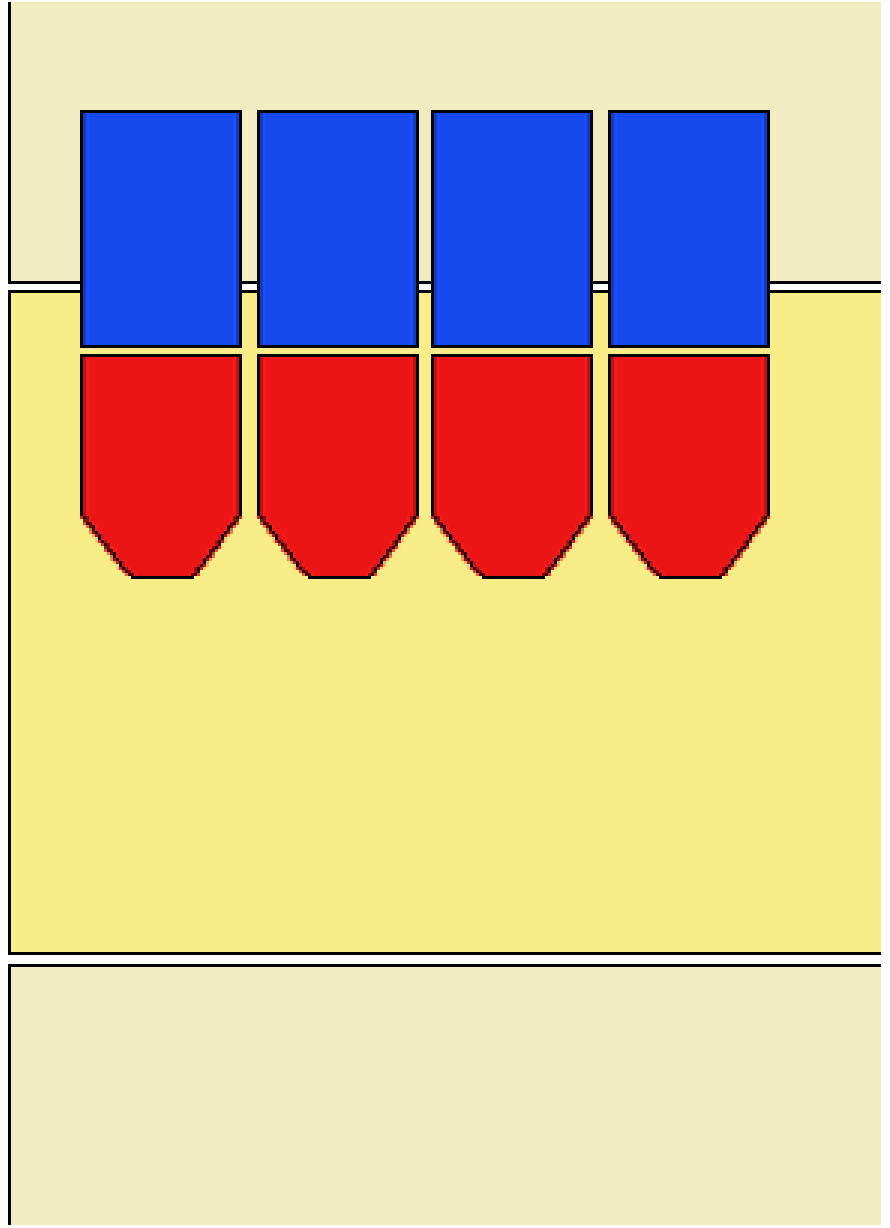
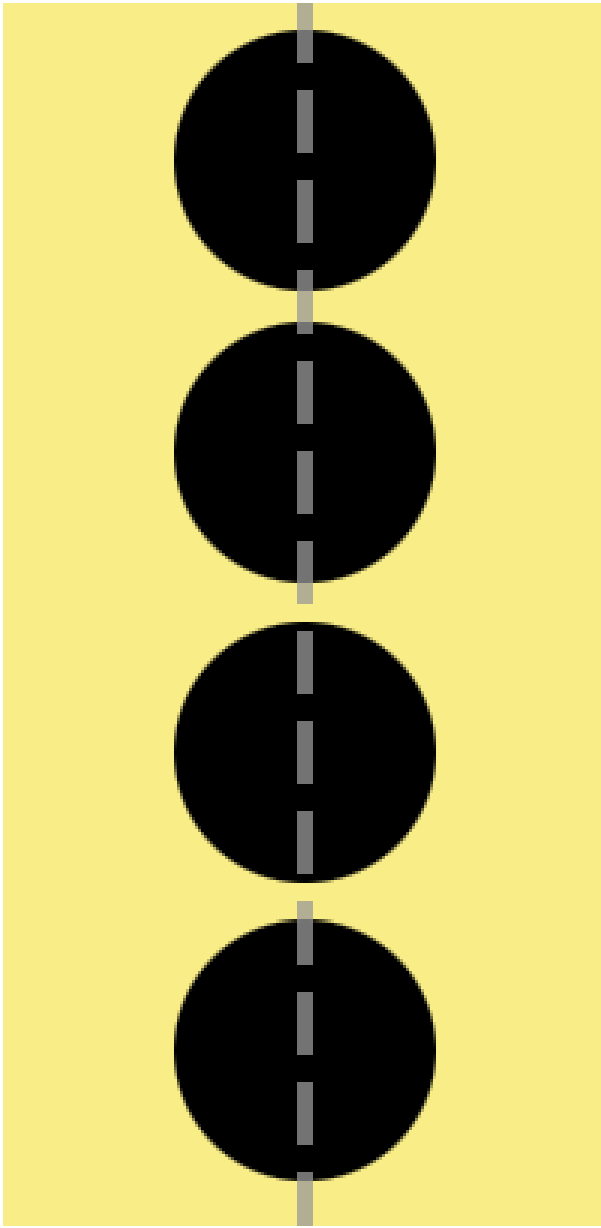


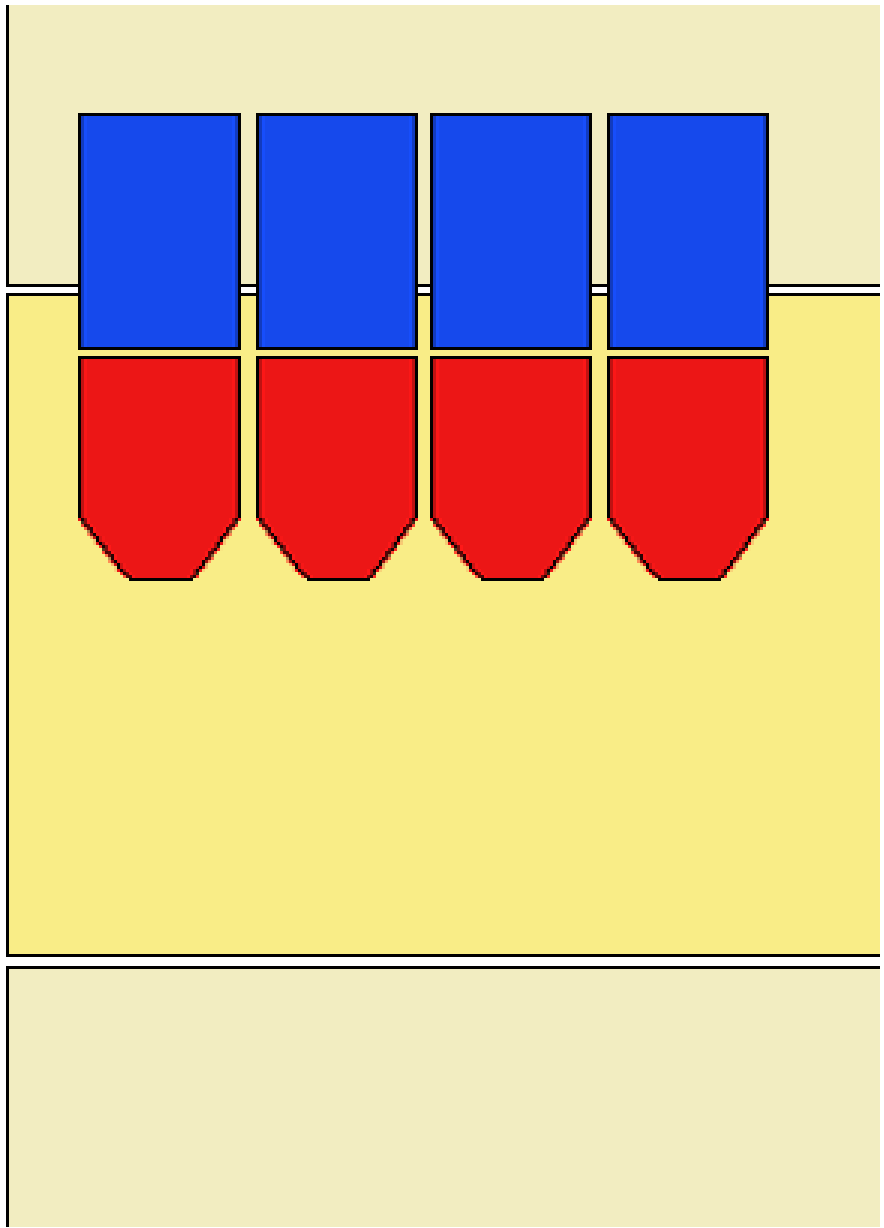
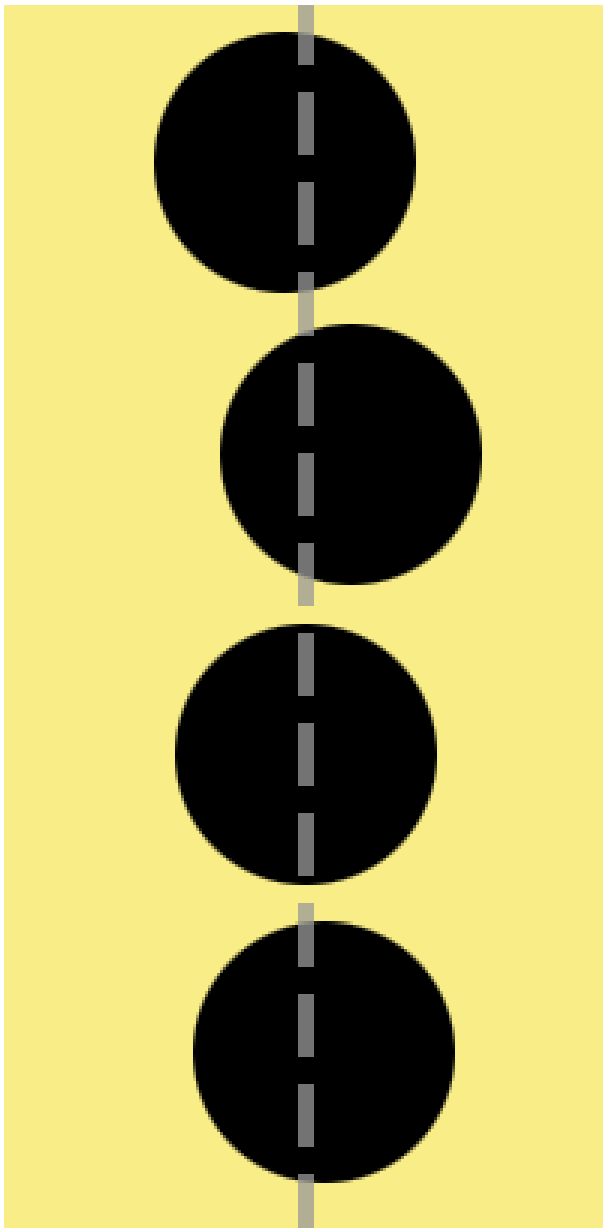


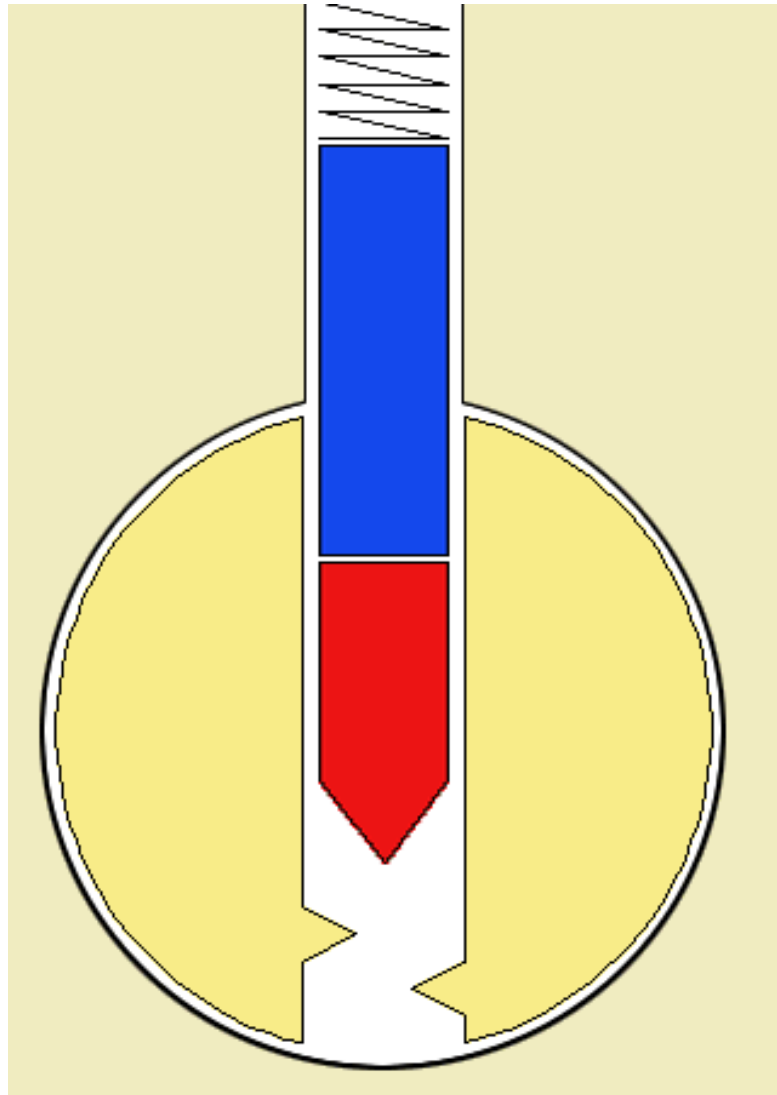
2. Most locks are wildly easy to pick

- Common faults
- Easily exploited
- Anyone can do it

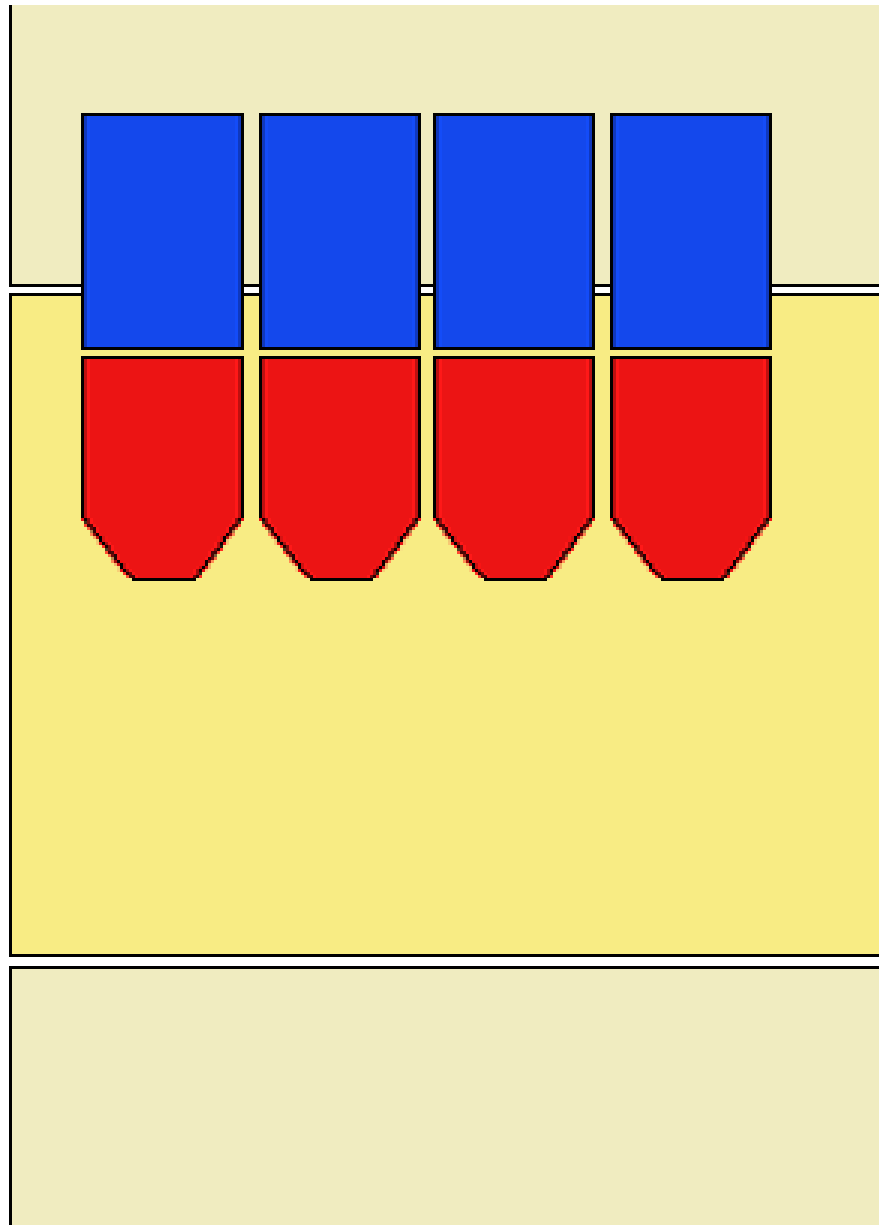








Picking

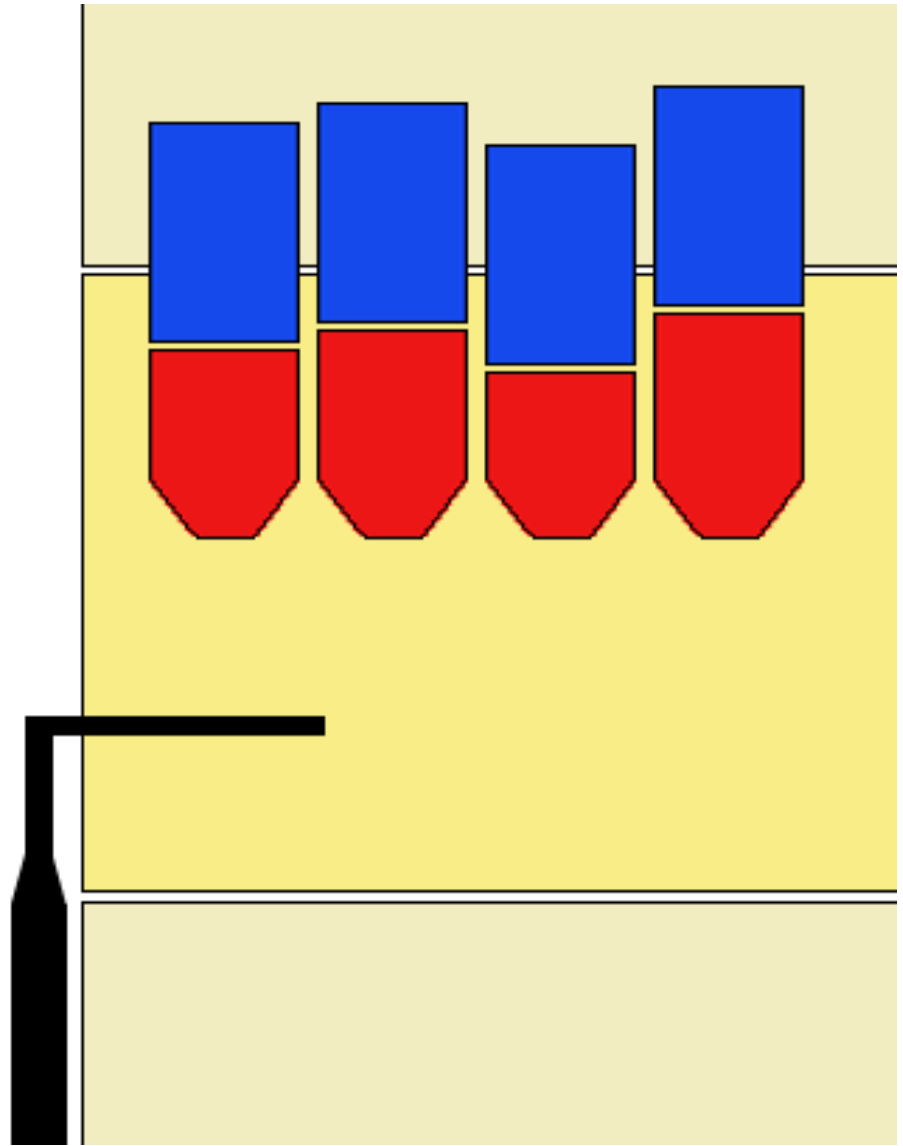


Demonstration

- **Everyone Cross Your Fingers**
- **Think “No Demonstration Effect”**
- **The Two Biggest Errors...**
 - Too much wrench pressure
 - Lifting pins too far up



Raking



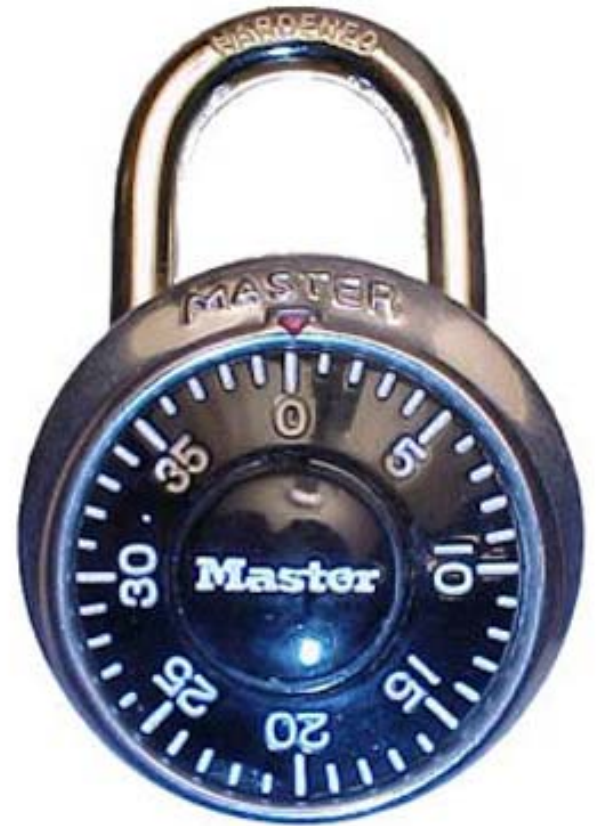
3. Unpickable doesn't mean invulnerable

- Combination instead of key
- Pins arranged in other formats
- Different keyway orientation



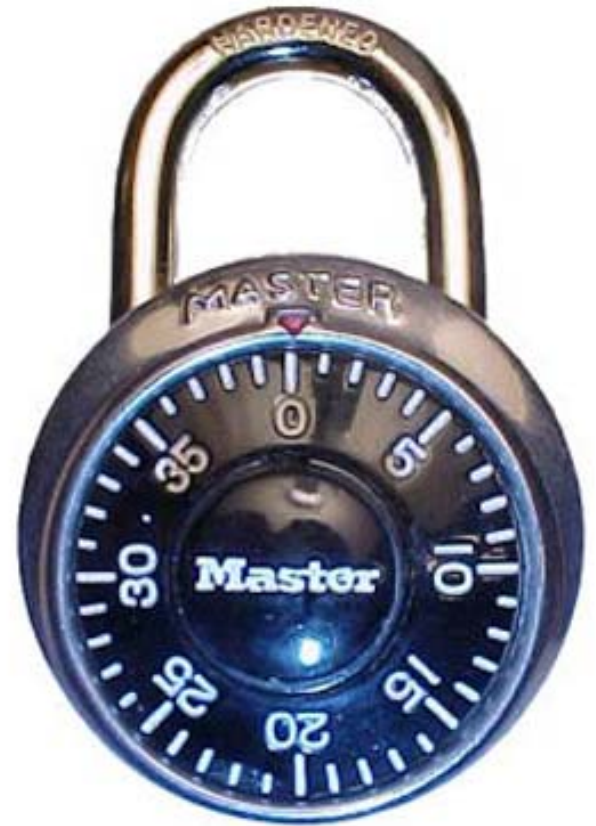
Combination Locks

- Show of Hands



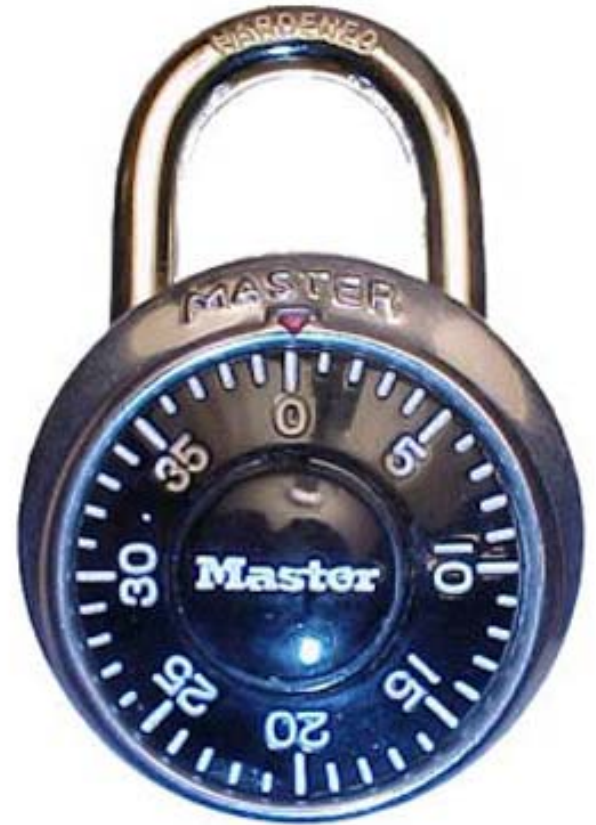
Combination Locks

- Show of Hands
- Immensely popular in the USA
 - Schools
 - Gyms
 - Etc.



Combination Locks

- Show of Hands
- Immensely popular in the USA
 - Schools
 - Gyms
 - Etc.
- These Locks Provide Essentially *Zero Security*

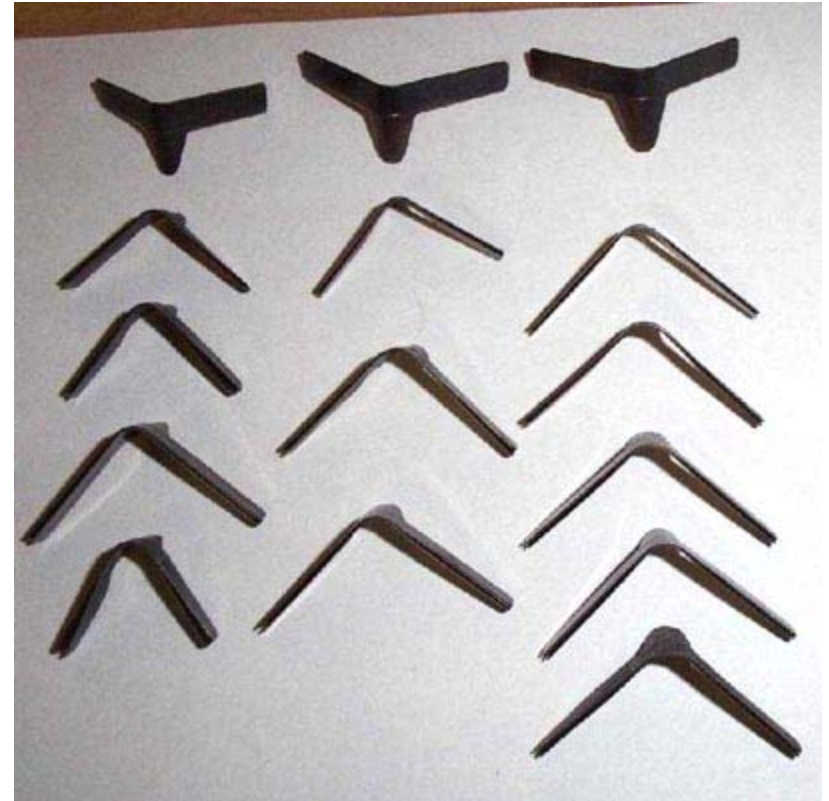






Padlock Shims

- **Simple**
- **Cheap**
- **Buy Online**
 - 20-pack for \$25
 - Shim stock metal
- **Homemade**
 - Aluminum Cans



Tubular Locks

- Still traditional pin stacks
- Pins simply arranged in unconventional pattern
- Need specialized tools (well... *sometimes*)



Low-tech Kryptonite bypass ([bic_pen.avi](#))

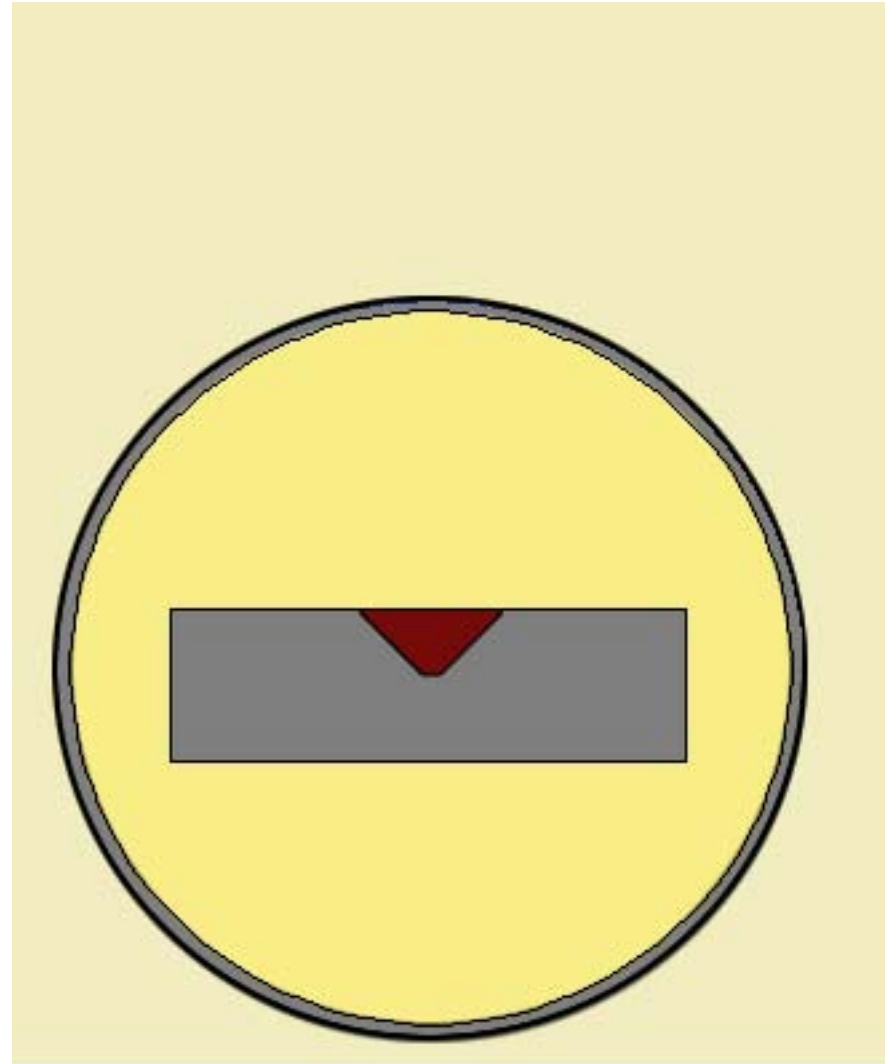
Dimple Locks

- Traditional pin stacks
- Horizontal keyway



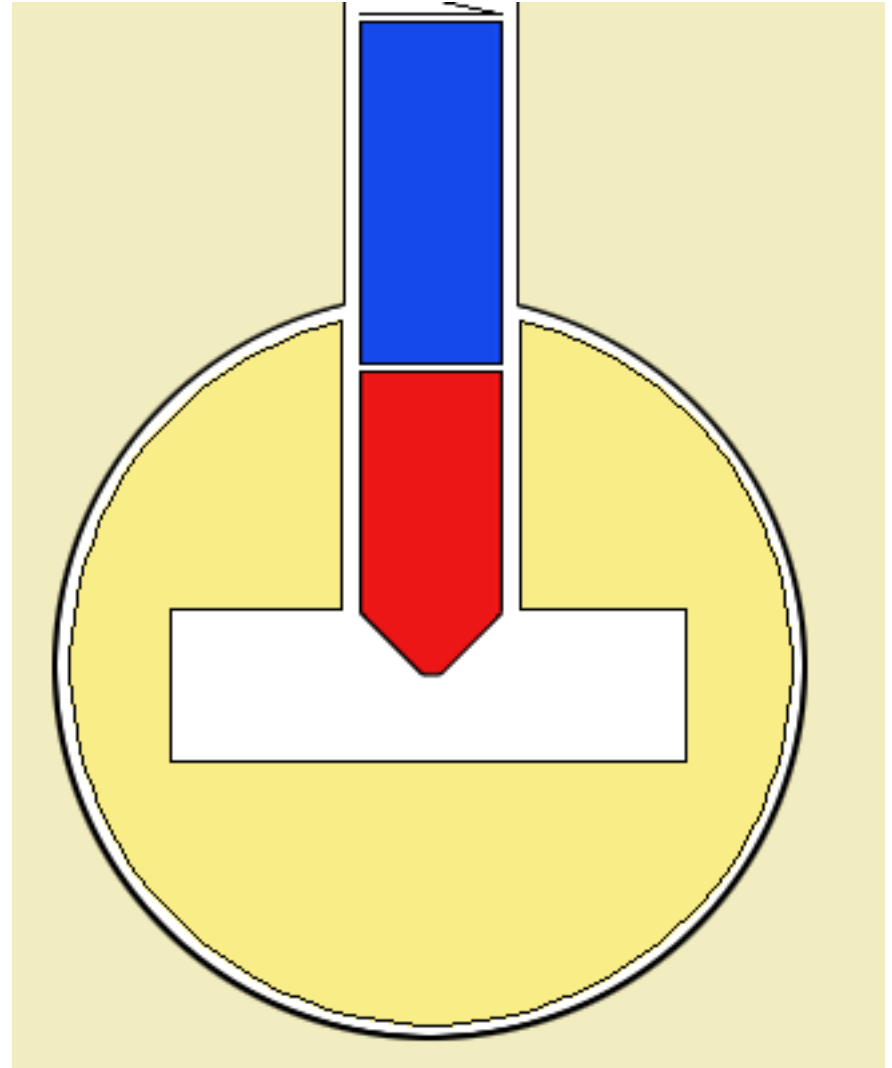
Dimple Locks

- Traditional pin stacks
- Horizontal keyway
- Nearly impossible to insert usual pick tools



Dimple Locks

- Traditional pin stacks
- Horizontal keyway
- Nearly impossible to insert usual pick tools
- Other means to bypass
 - Impressioning
 - Bump keying



Barry Wels & Laz impressioning a dimple lock (dimple.avi)

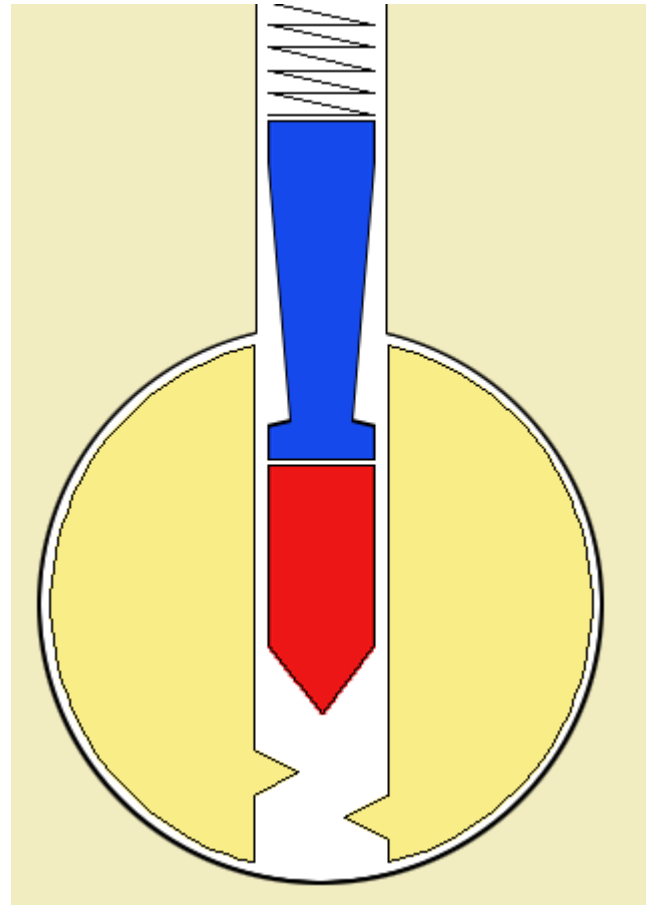
4. Minor changes make a big difference

- Specialized pins
- Unshimable padlocks



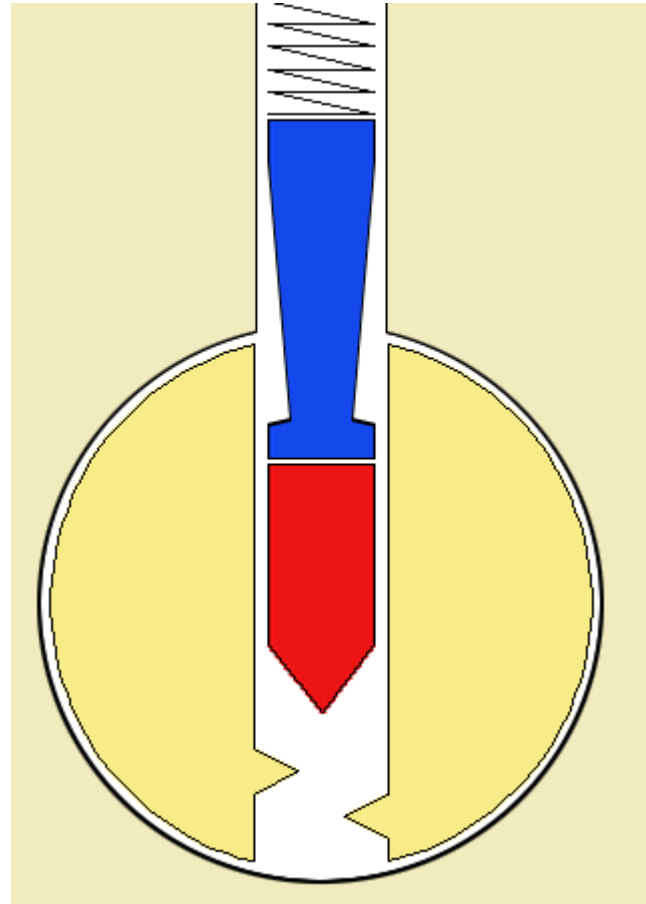
Pick-Resistant Pins

- Mushroom



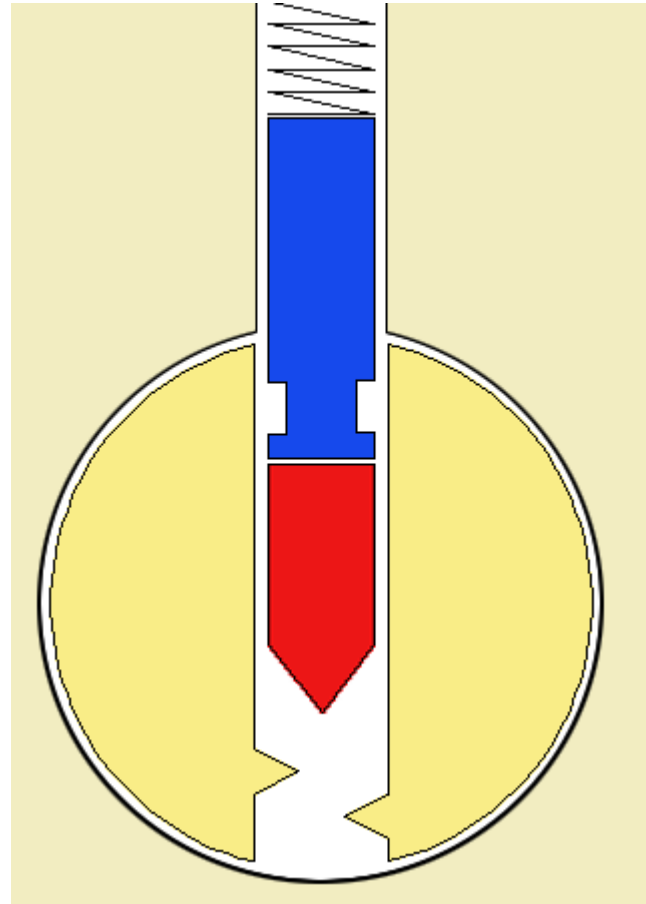
Pick-Resistant Pins

- Mushroom



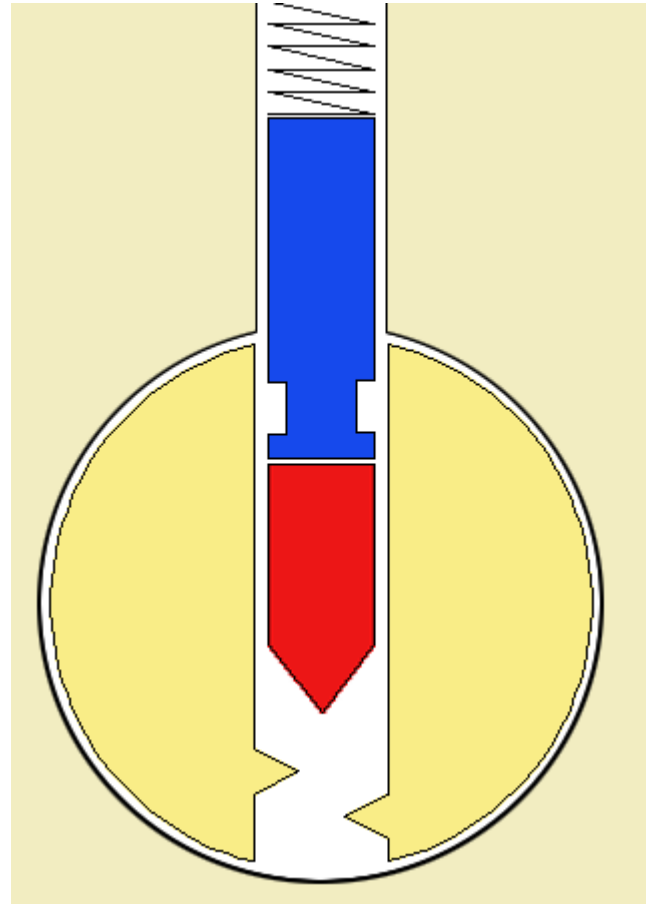
Pick-Resistant Pins

- Mushroom
- Spool



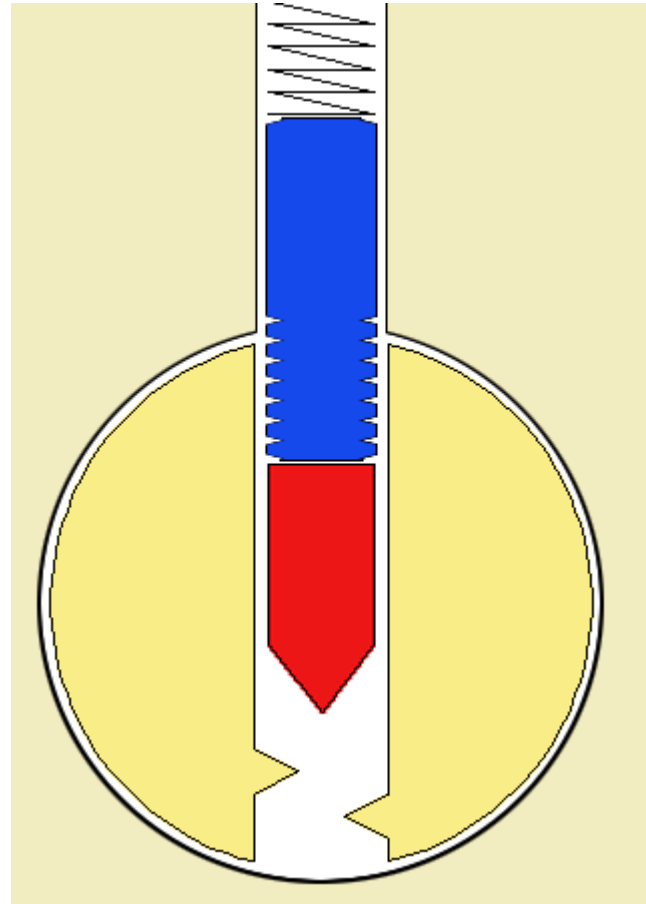
Pick-Resistant Pins

- Mushroom
- Spool



Pick-Resistant Pins

- Mushroom
- Spool
- Serrated



Europe Raises the Bar

TrioVing®

A14
10041

Låssylinder, oval

- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modulås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.



Se også vår hjemmeside
www.trioving.no



Europe Raises the Bar

TrioVing® A14
10041

Låssylinder, oval

- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modulås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.

TrioVing 5520 **TrioVing 5537**



Brukbare verktøy:



(5537)
Skrujern pzd2

(5520)
Skrujern spor



Se også vår hjemmeside
www.trioving.no



Europe Raises the Bar

A14
10041

TrioVing®

Låssylinder, oval

- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modullås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.

TrioVing 5520 **TrioVing 5537**



Brukbare verktøy:



(5537)
Skrujern pzd2



(5520)
Skrujern spor



Se også vår hjemmeside
www.trioving.no



Europe Raises the Bar

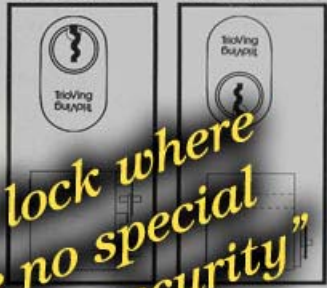
A14
10041

TrioVing®

Låssylinder, oval

- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modullås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.

TrioVing 5520 TrioVing 5537




“Use this lock where there are no special demands for security”

Brukbare verktøy

(5537)
Skrujern pzd2

(5520)
Skrujern spor

Se også vår hjemmeside
www.trioving.no



7 030680 000543

Europe Raises the Bar



Un-Shimmable Padlocks

- Collar / Boot
- Double-Ball Mechanism
- Key-Retaining Locks
 - Less Convenient
 - Less Popular
- Can still have combination dials
- Size doesn't always equal security
 - Resistance to Brute Force
 - Not Always Resistant to Finesse



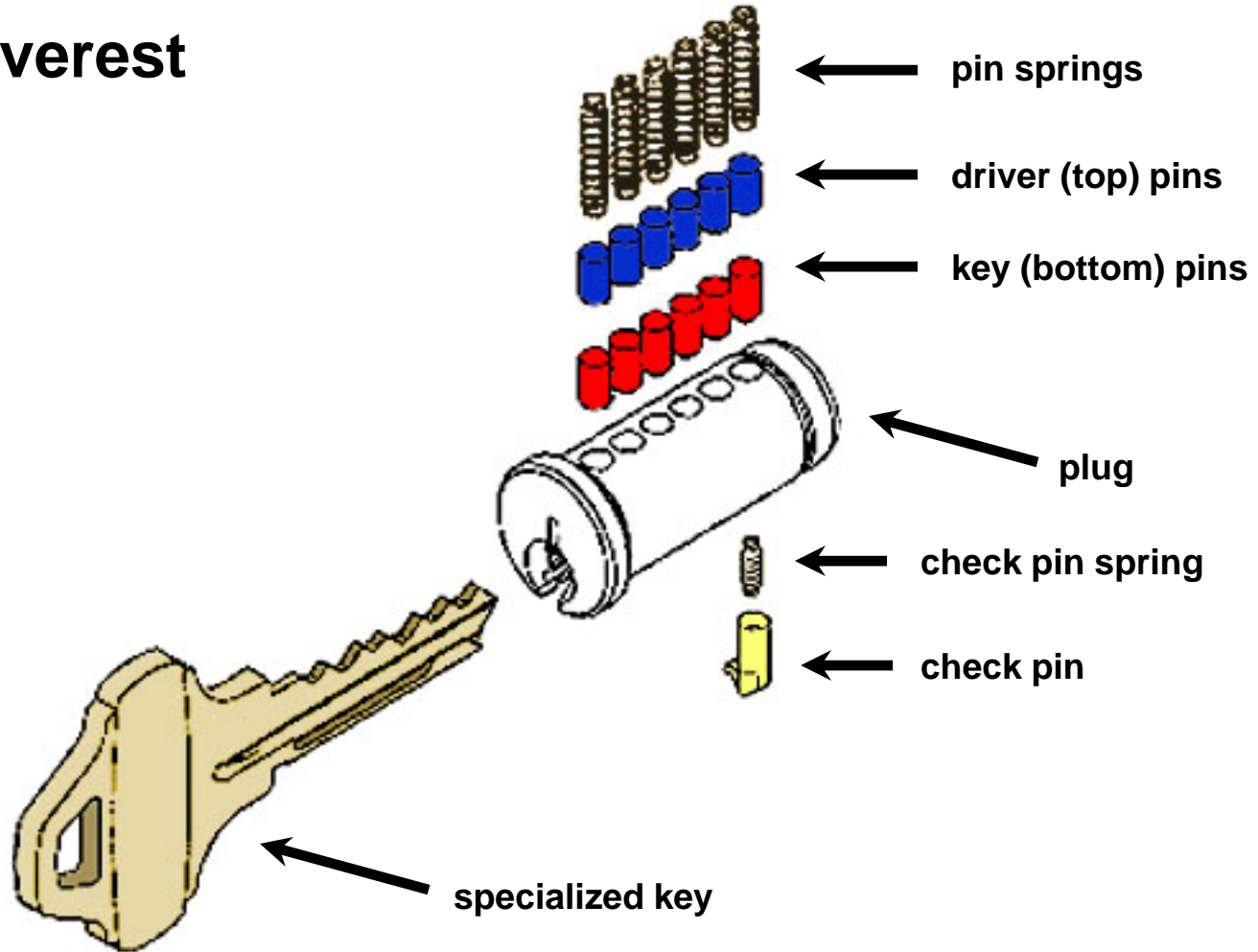
5. Advanced features aren't a panacea

- Sidepin... the industry's first attempt
- Sidebars... good and bad
- Mul-T-Lock dimple system
- Abloy's rotating disks



Side Pin

Schlage Everest



Side Pin

Schlage Everest



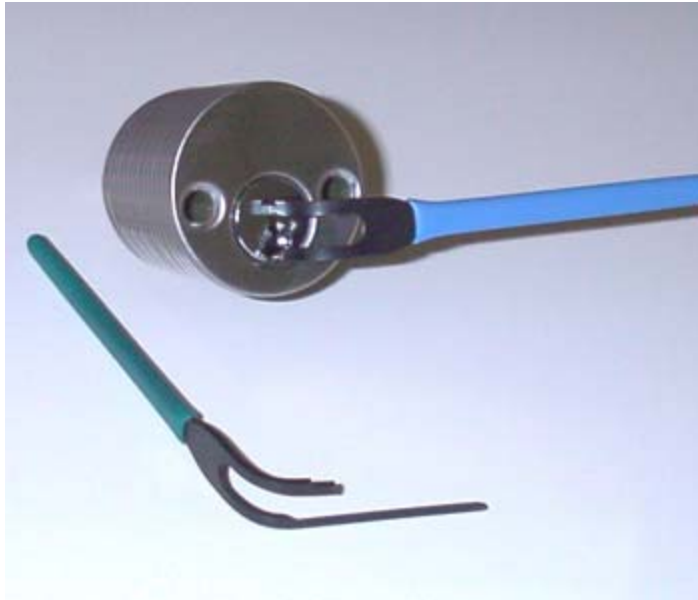
Side Pin

Schlage Everest



Side Pin

Schlage Everest



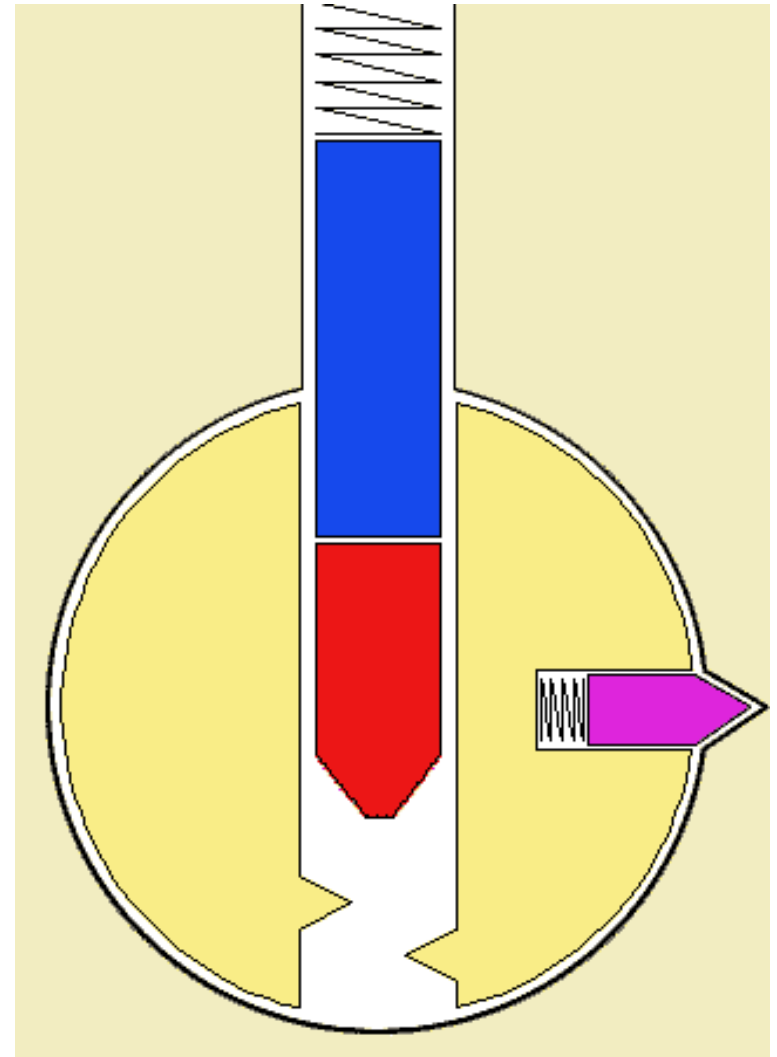
specialized “finger wrench”



modified Everest key

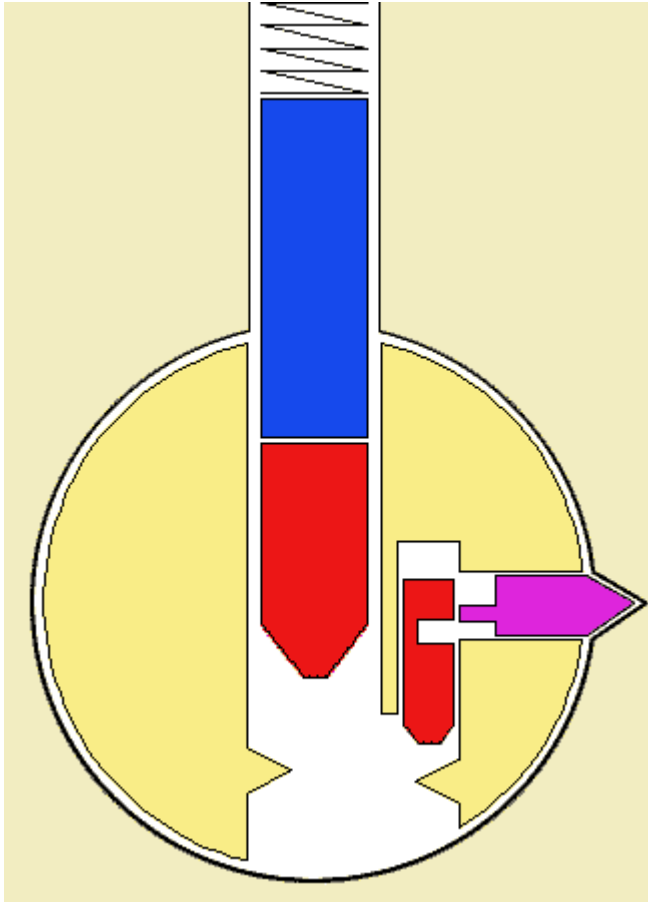
Side Bars

- Similar to side pins
- Restrict plug movement
- Harder to pick than pin stacks



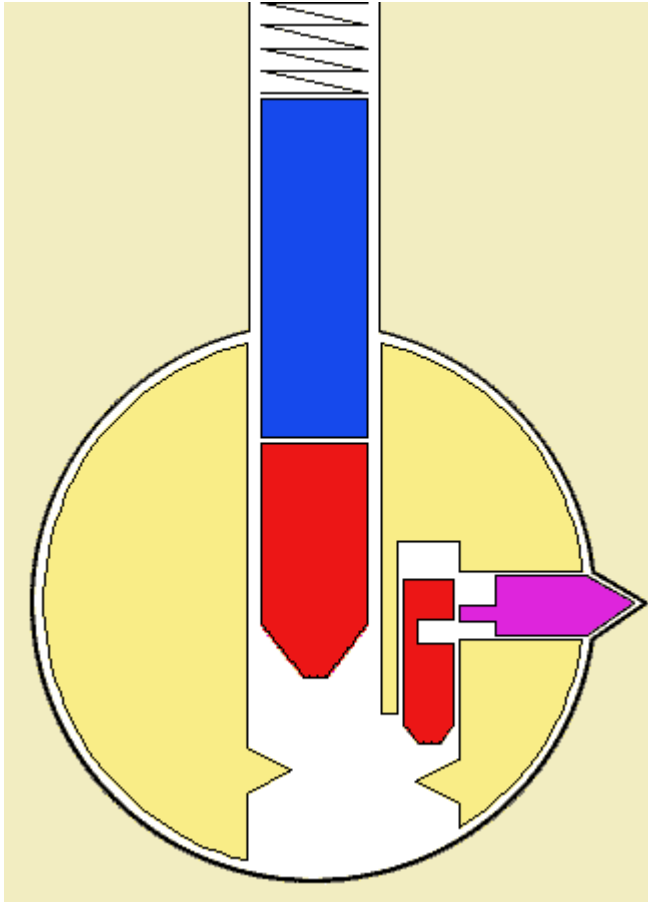
Side Bar

Finger Pins



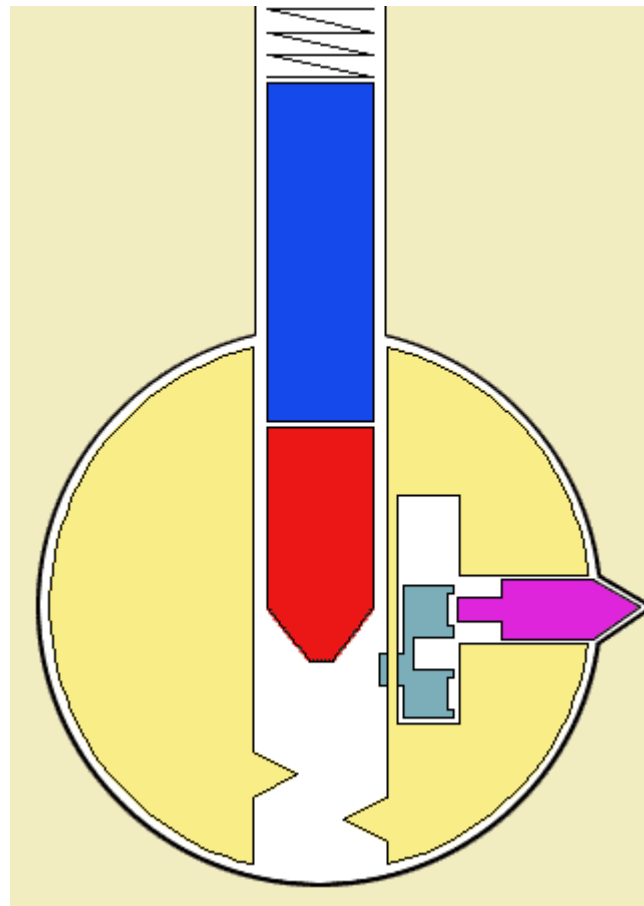
Side Bar

Finger Pins



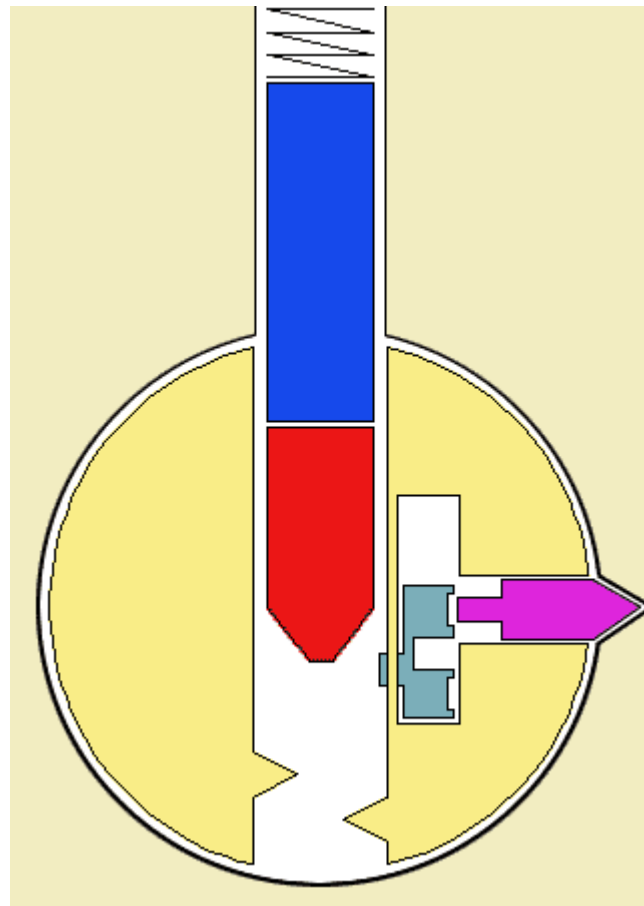
Side Bar

Sliders



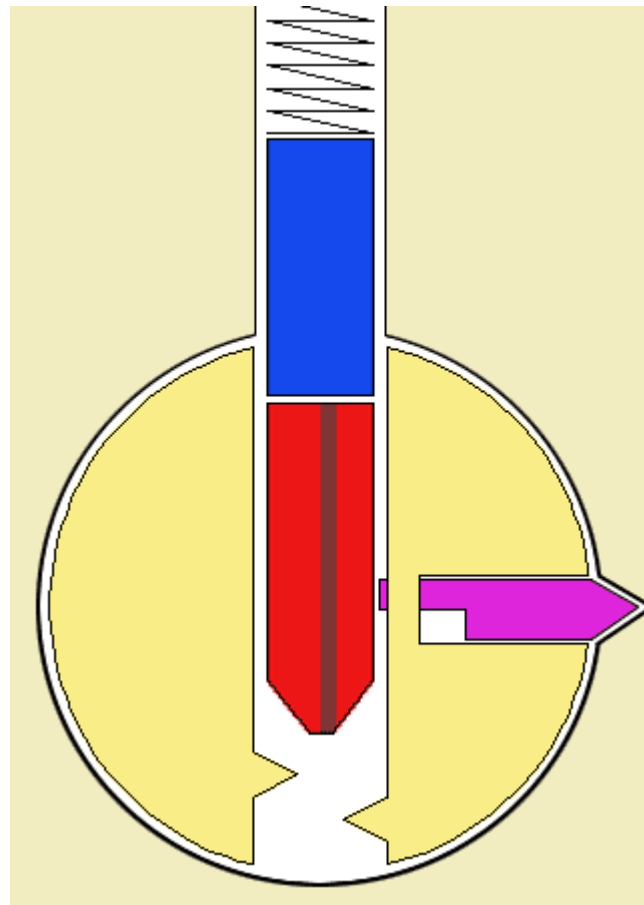
Side Bar

Sliders



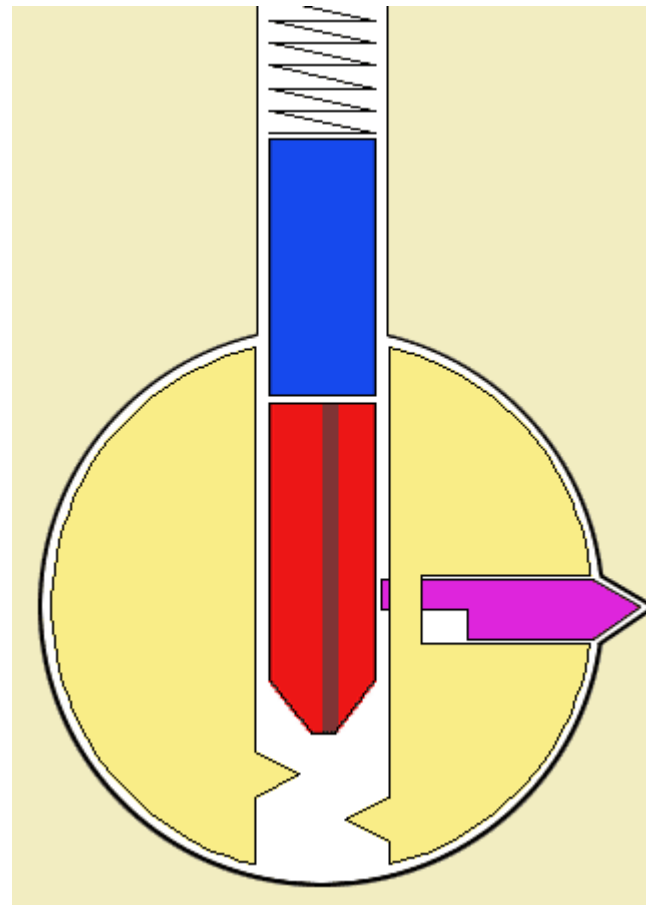
Side Bar

Rotating Pins



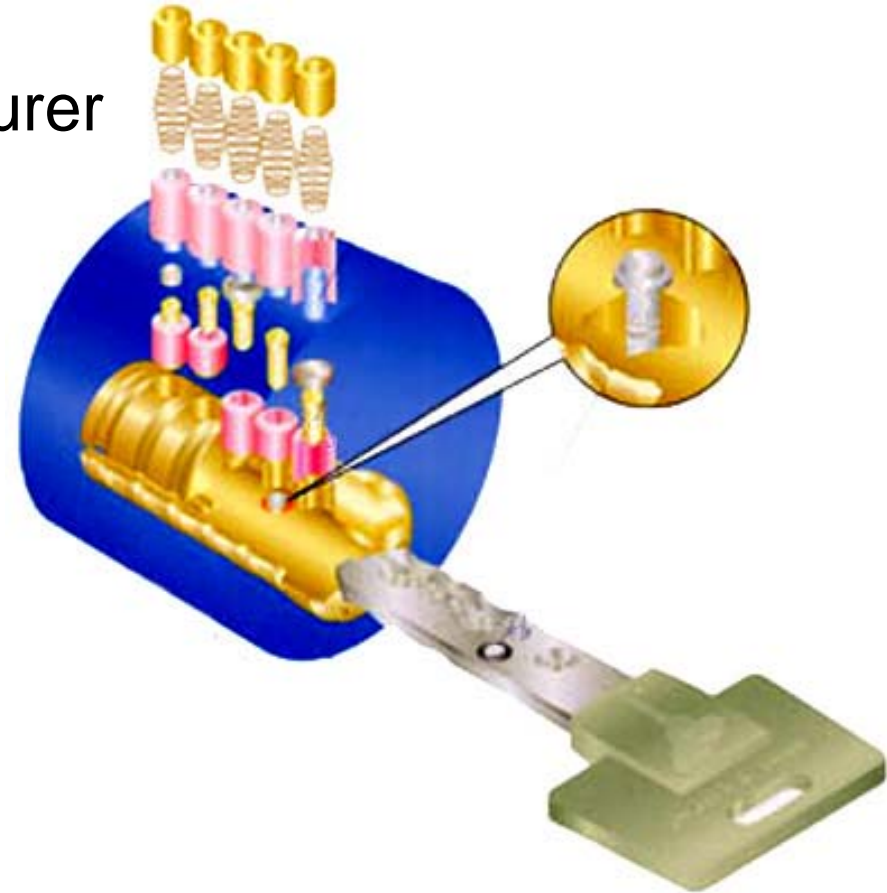
Side Bar

Rotating Pins



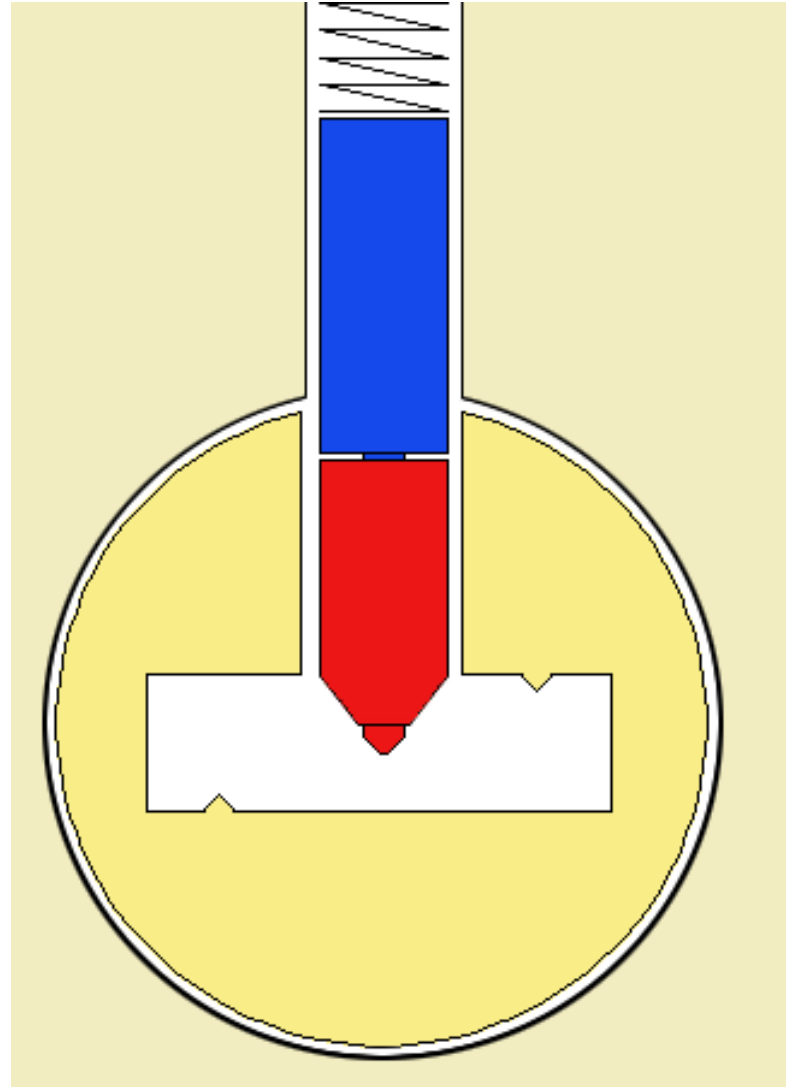
Advanced Dimple Lock

- **Mul-T-Lock**
 - Developer & Manufacturer
 - Patent Holder
 - Exclusive Distributor
- **Specialized Design**
 - Pins Within Pins
 - Can't Impression



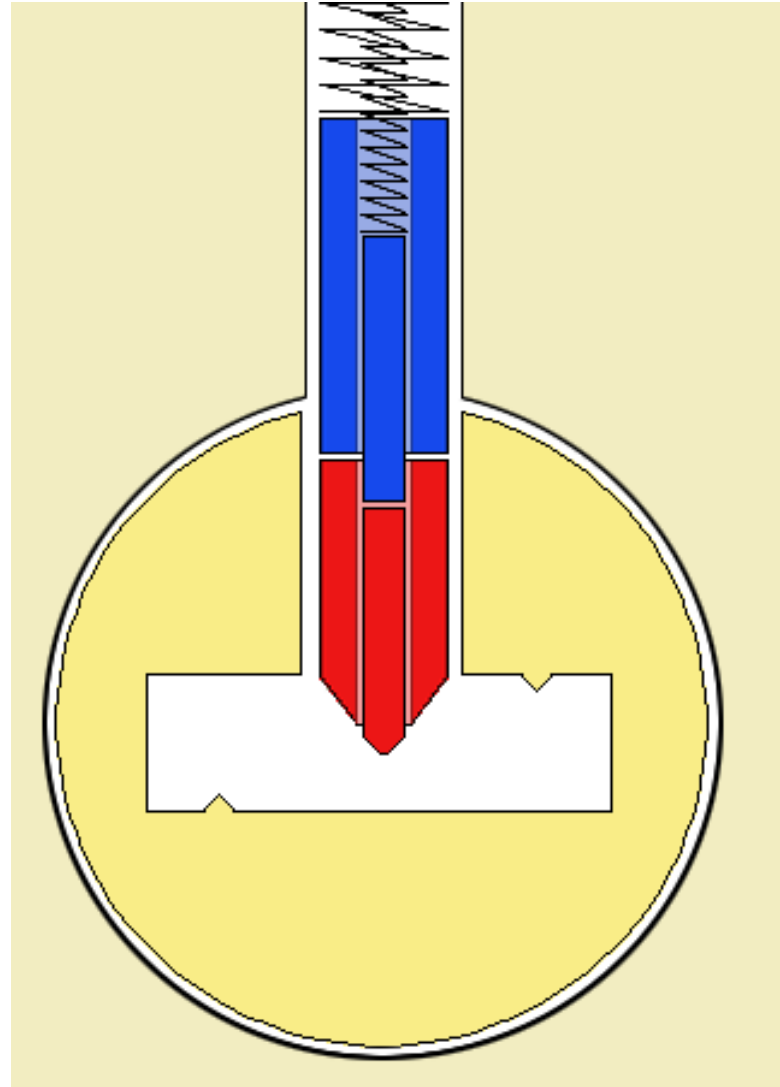
Mul-T-Lock

- Pins within pins



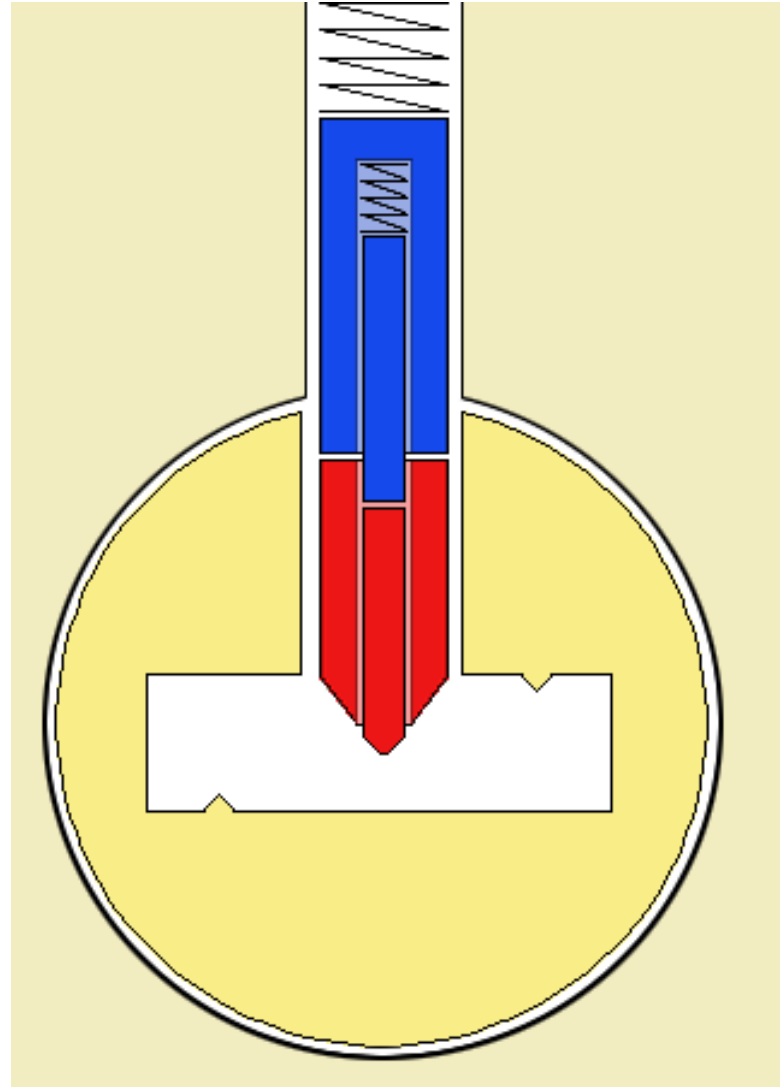
Mul-T-Lock

- Pins within pins
- Imagine the inside

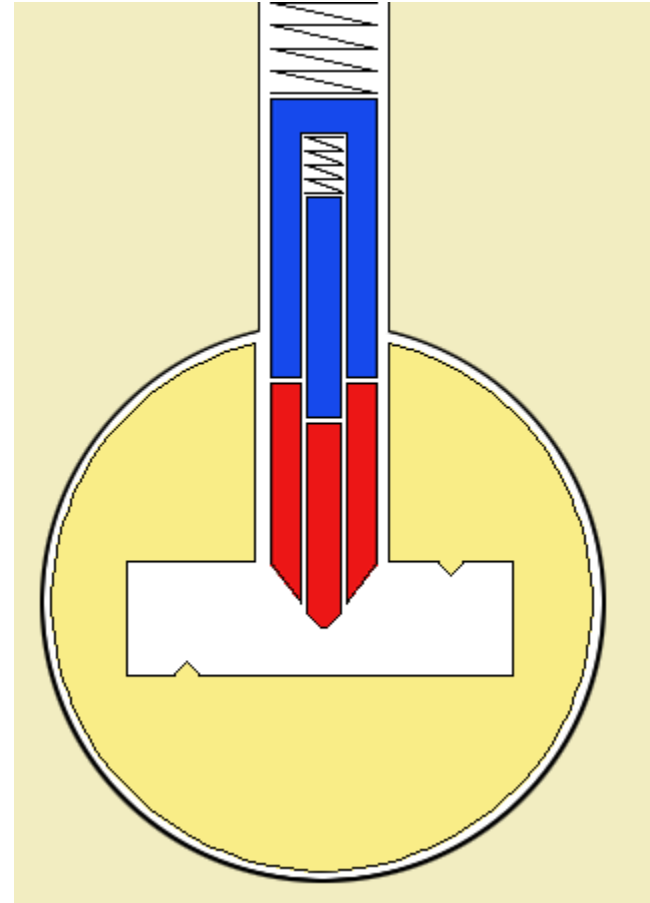
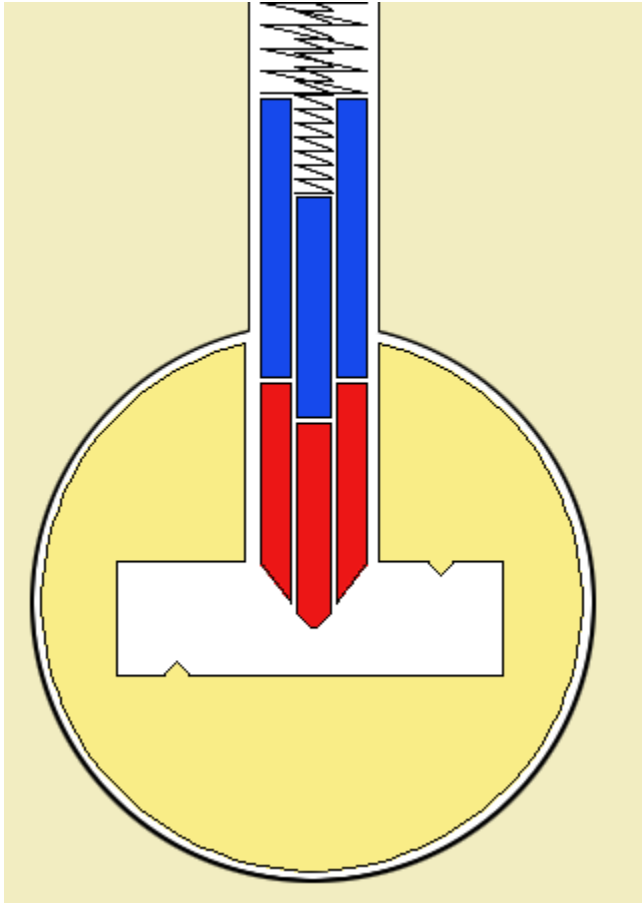


Mul-T-Lock

- Pins within pins
- Imagine the inside
- In fact, *this* is the actual mechanism



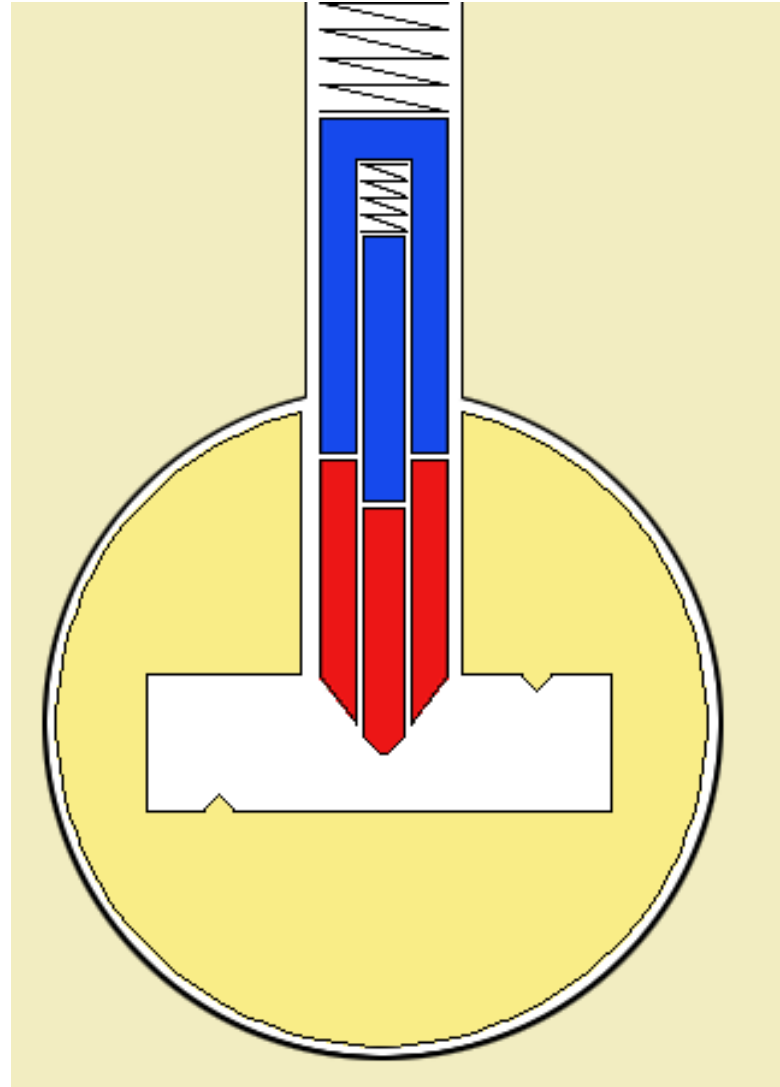
Mul-T-Lock



see the difference now?

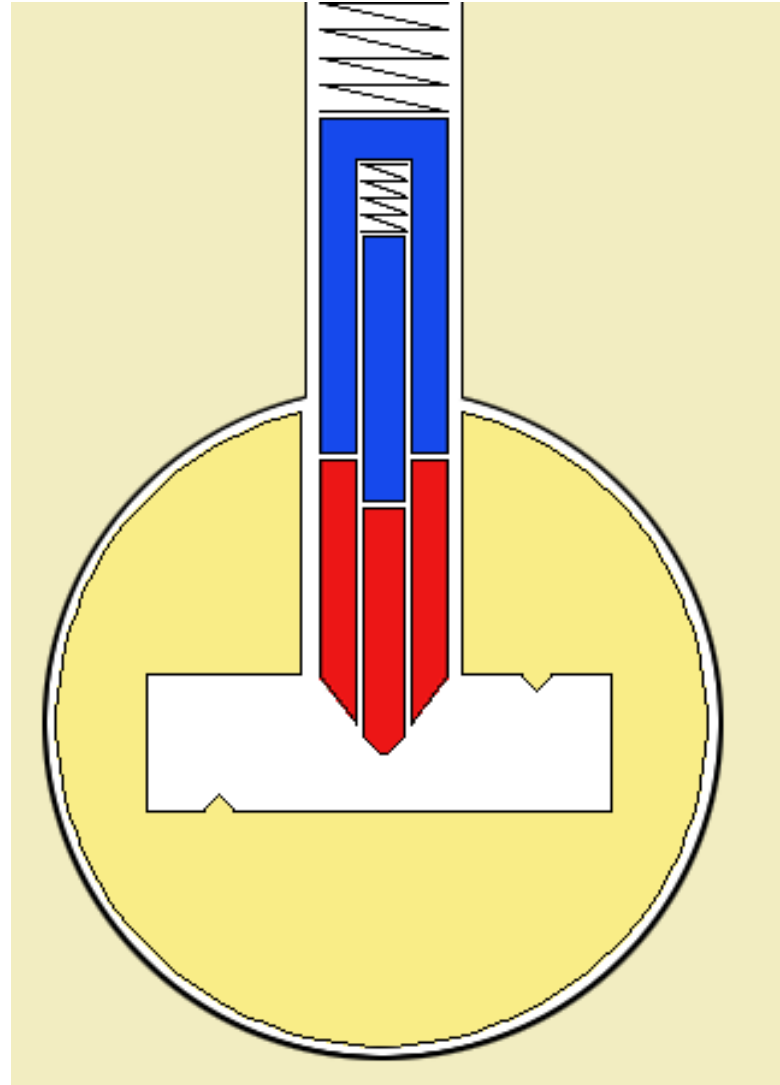
Mul-T-Lock

- Standard Operation



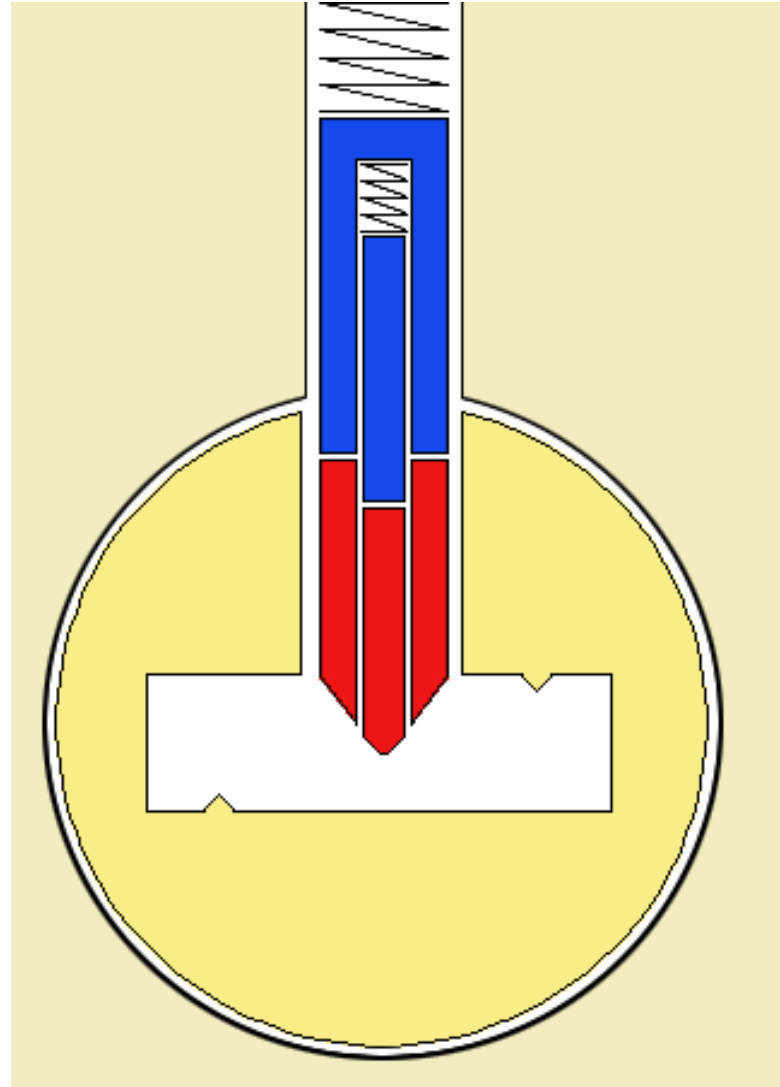
Mul-T-Lock

- Standard Operation
- Overlifting



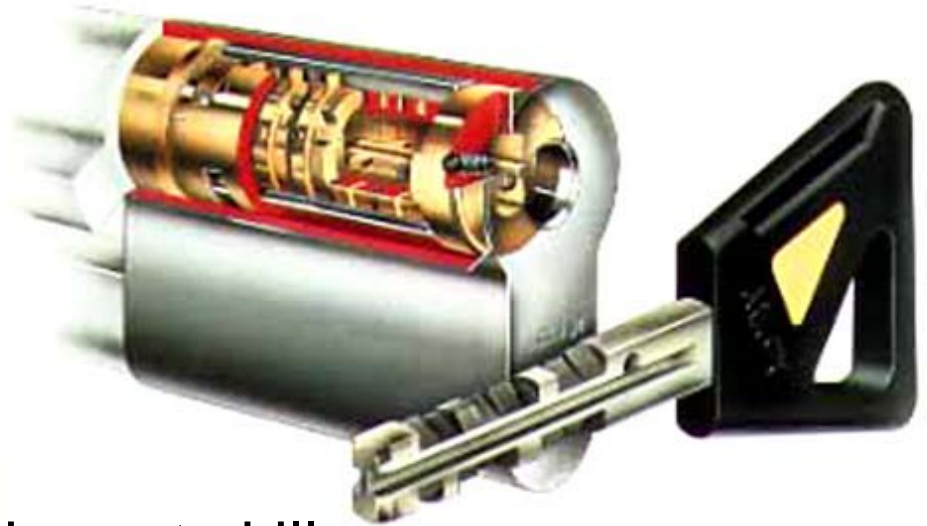
Mul-T-Lock

- Standard Operation
- Overlifting
- Michaud Attack



Rotating Disks

- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required



Rotating Disks

- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required
- **Falle Tool**
 - Manipulates disks individually
 - Decodes cut orientation
 - Numerical key values







Barry Wels picking a rotating disk lock with Mike Glasser (rotating_disk.avi)

6. Adding electricity isn't magical

- **Hotel safes**
- **Deadbolts**
- **Access control systems**
 - Magnetic door locks
 - Passive IR sensors
 - The Wiegand pitfall



-  Malaysian Hotel (electronic_safe_spiking.avi)
-  Major Malfunction (majormal-paperclip.avi)
-  Winkhaus Blue Chip (winkhaus_long.avi)
-  Mul-T-Lock CLIQ System (cliq.avi)

A problematic access control door

- Magnetic lock



A problematic access control door

- Magnetic lock
- Large gap



A problematic access control door

- Magnetic lock
- Large gap
- IR Sensor



Zac Franken... the Gecko project



7. Safe locks vary as widely as door locks

- Mechanisms
- Certifications
- Resistance to other conditions
- Amazing electronic models



Safes

- **Mechanism Operation**
 - Wheels, Gates, & a Fence
 - Direct Entry Fence vs. Nose & Cam
- **Insurance Ratings**
 - Underwriters' Labs (TL, TRTL, TXTL + ##)
- **Fire Safes**
 - Often terribly weak hardware
 - Also not typically rated for electronic media
- **Compromise**
 - Manual or Robotic Manipulation
 - Manipulation-Proof Safes (S&G 8400)
 - Electronic Mas-Hamilton X-07 & X-09



8. Bump keying is a real problem...

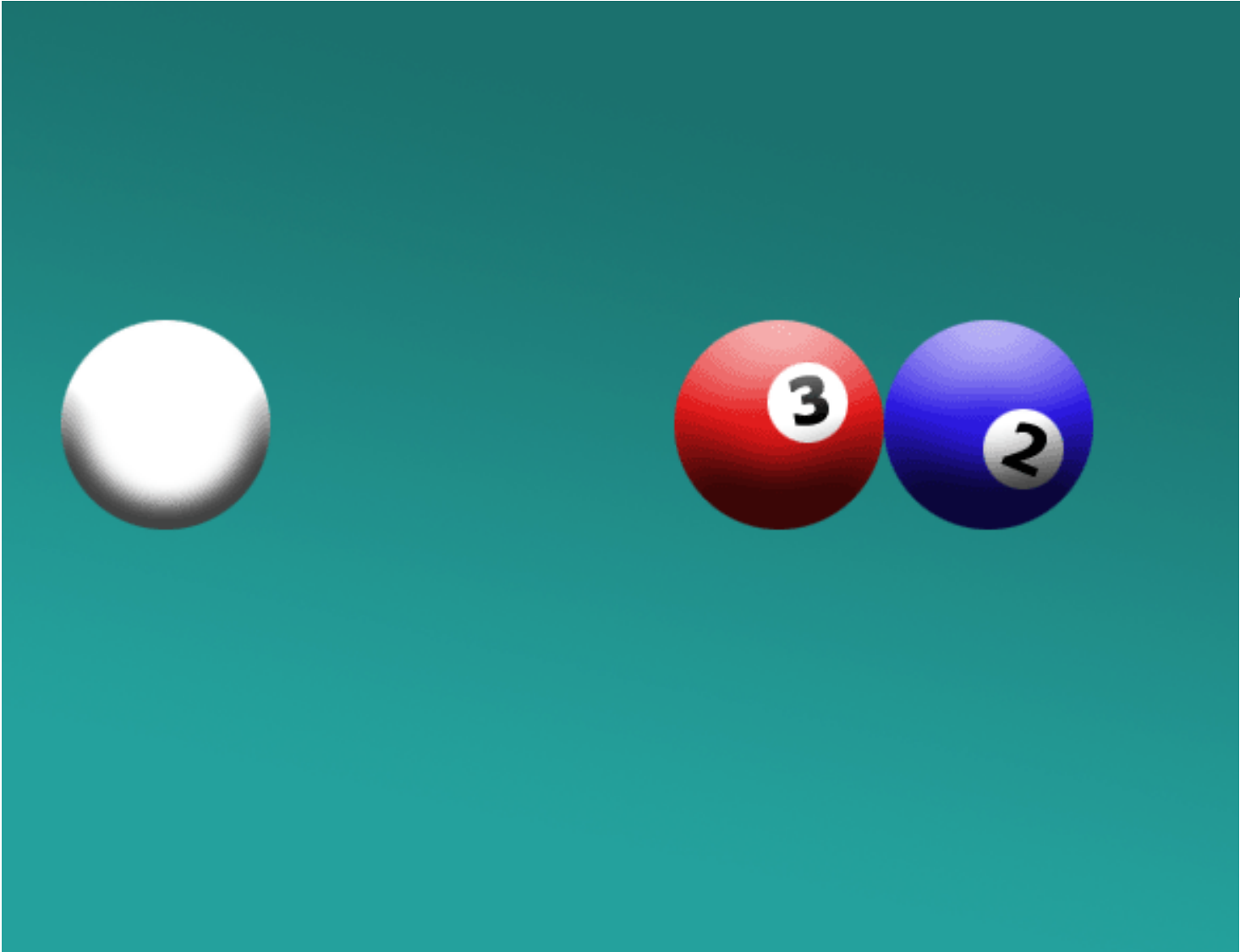
... but one with real solutions

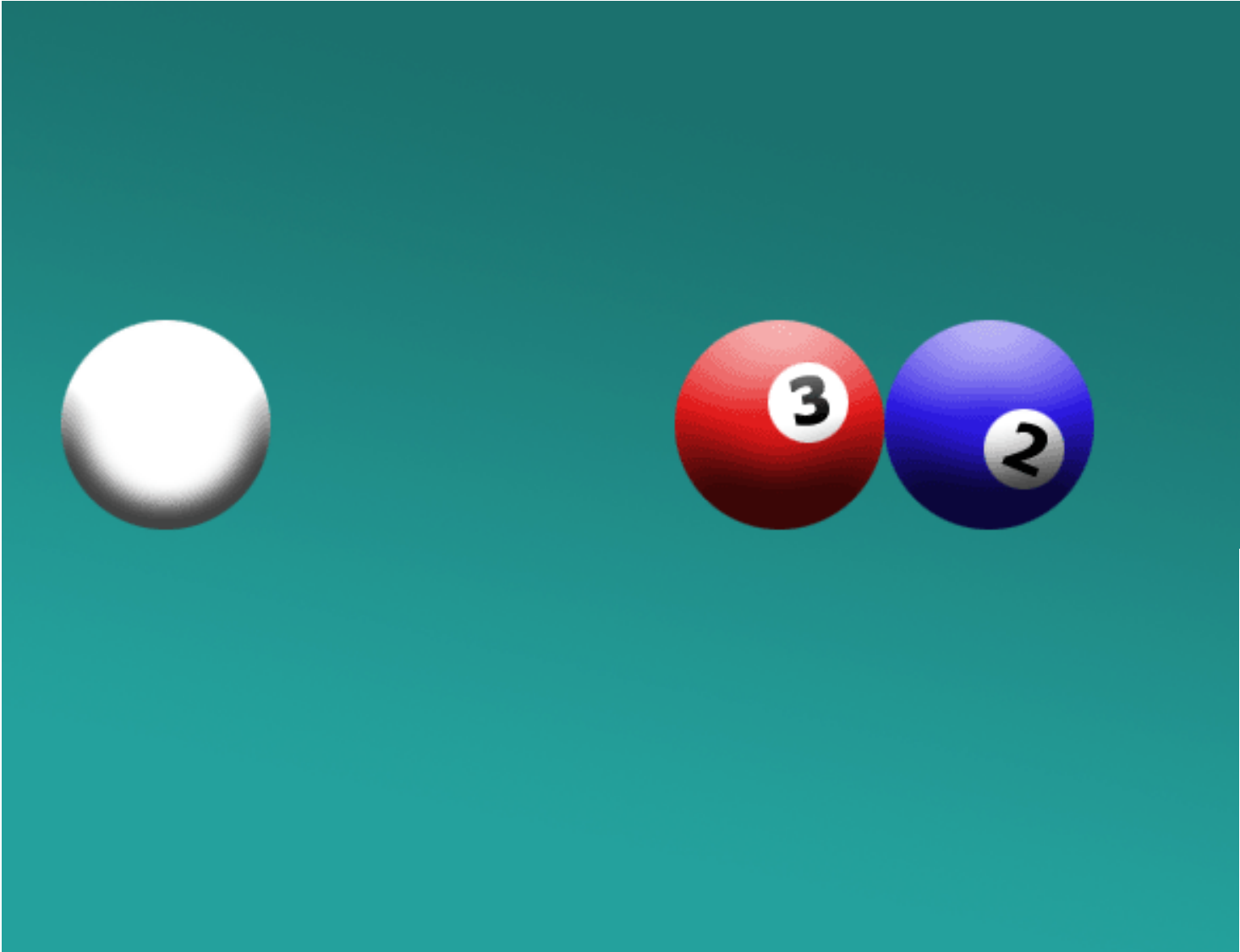


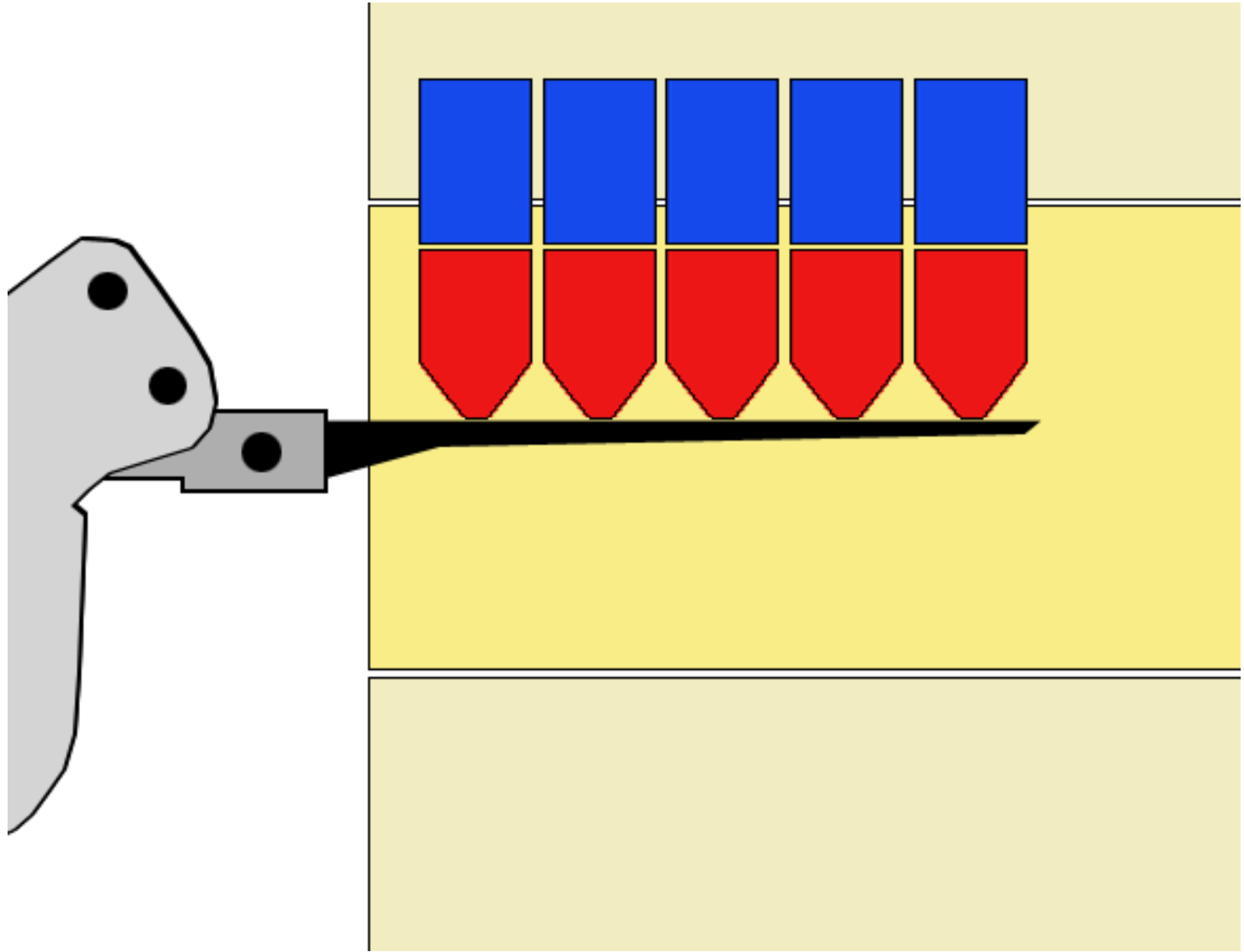
The “Bump Key” Attack

- Popping a lock open with a special key
- Takes little skill, almost no training, no special tools
- **Vast number of locks are vulnerable**
 - The media (and public) is finally taking notice
- **Exploit closely related to physics of a pick gun**
 - Best explained via billiard ball analogy...

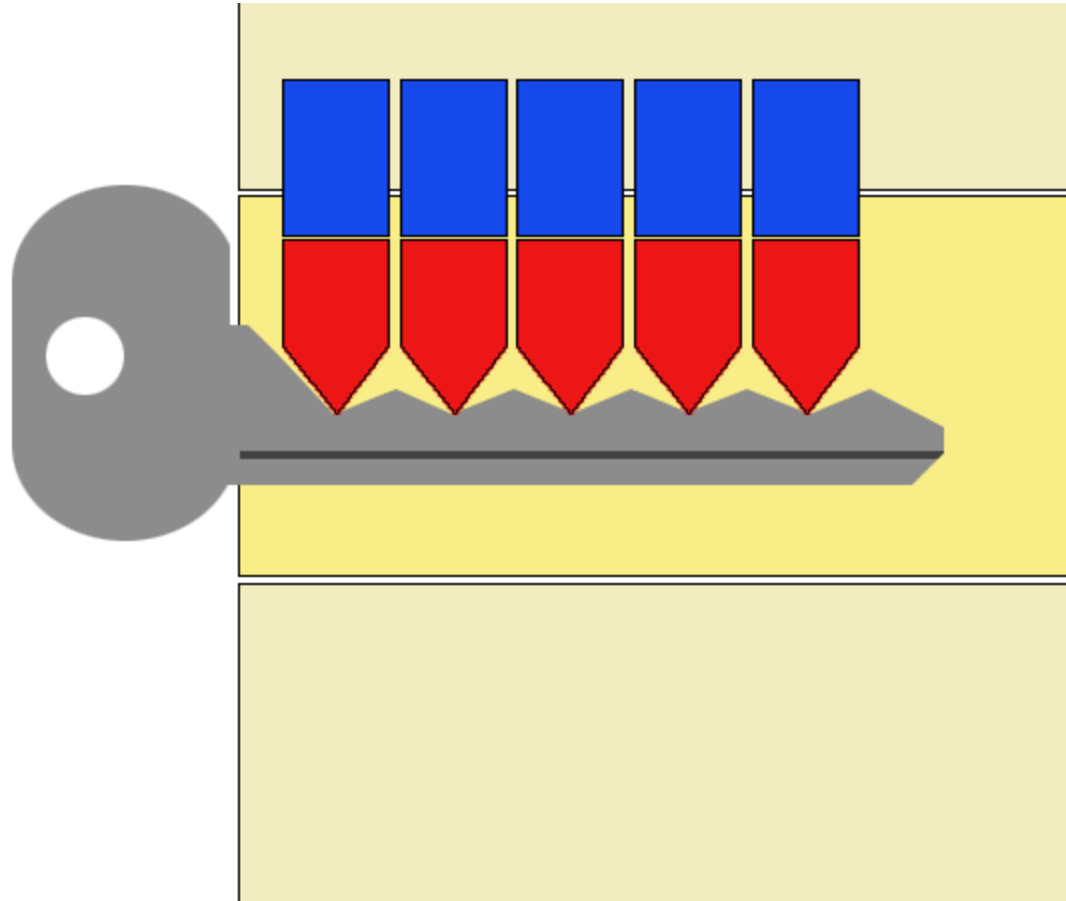




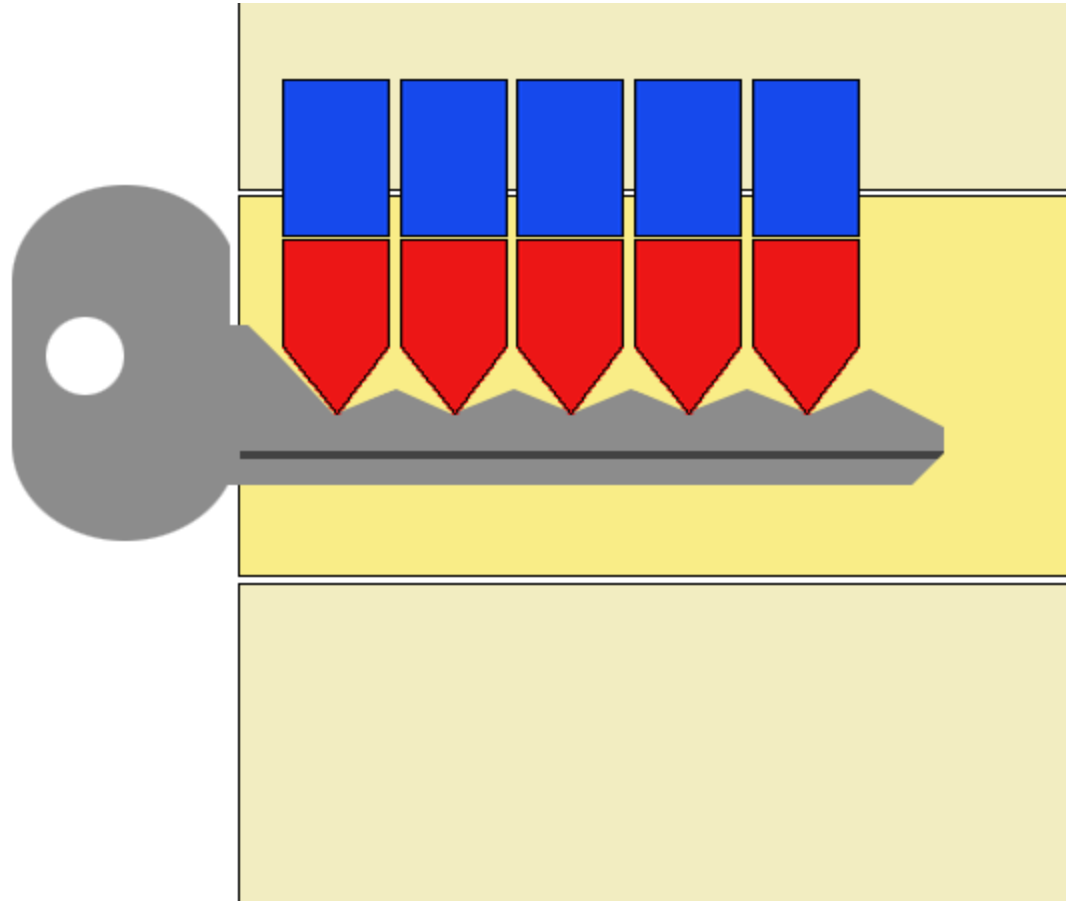




The “Bump Key” Attack



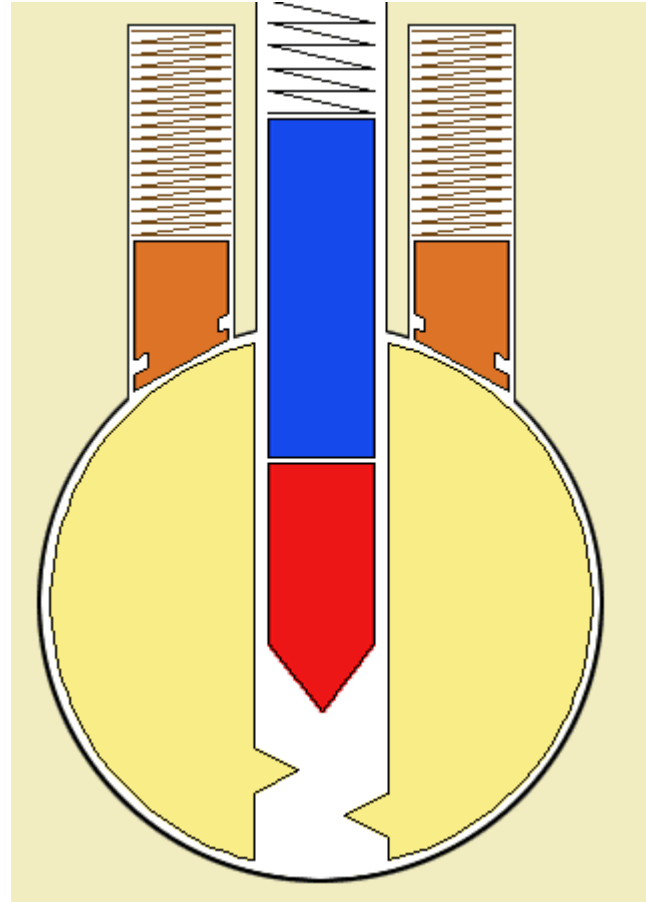
The “Bump Key” Attack



Countermeasures to Bumping

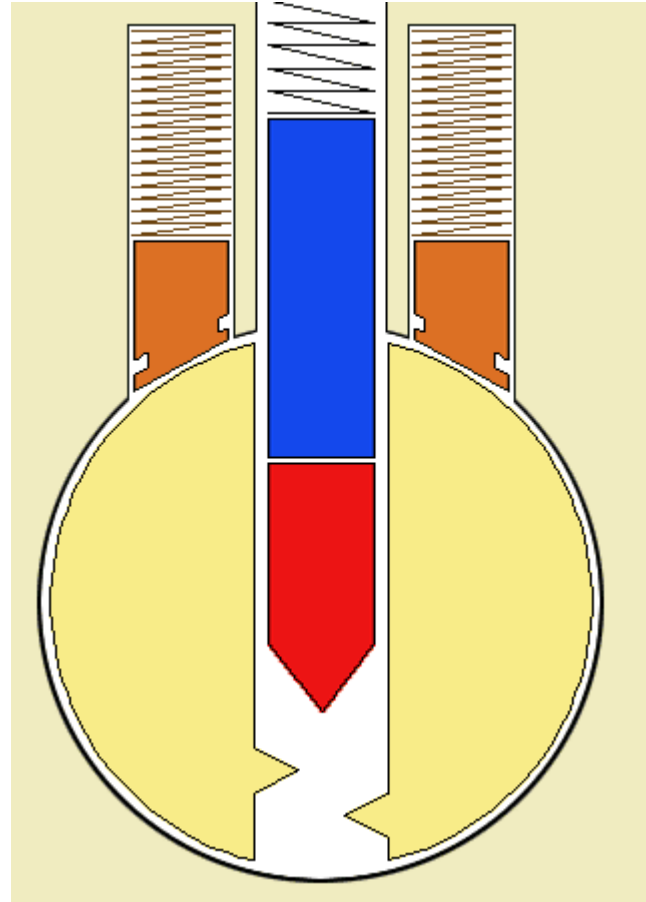
- **Certain High Security Mechanisms**
 - Sidebars in Schalge Primus
 - Slider-based sidebars in Evva & Scorpion
 - Pins Within Pins (newer Mul-T-Lock models)
 - Rotating Disk locks (Abloy & clones)
- **Other High Security Locks Don't Help As Much**
 - Assa V10 Twin is “exploitable” geographically
 - It is *theoretically possible* that Medeco locks could be bumped (given adequate knowledge beforehand)
 - There is a risk of information leakage in mastered systems
- **New Approaches**
 - Trap Pins
 - Shallow Drilling
 - Top Gapping
 - Fluids & Gels

Trap Pins



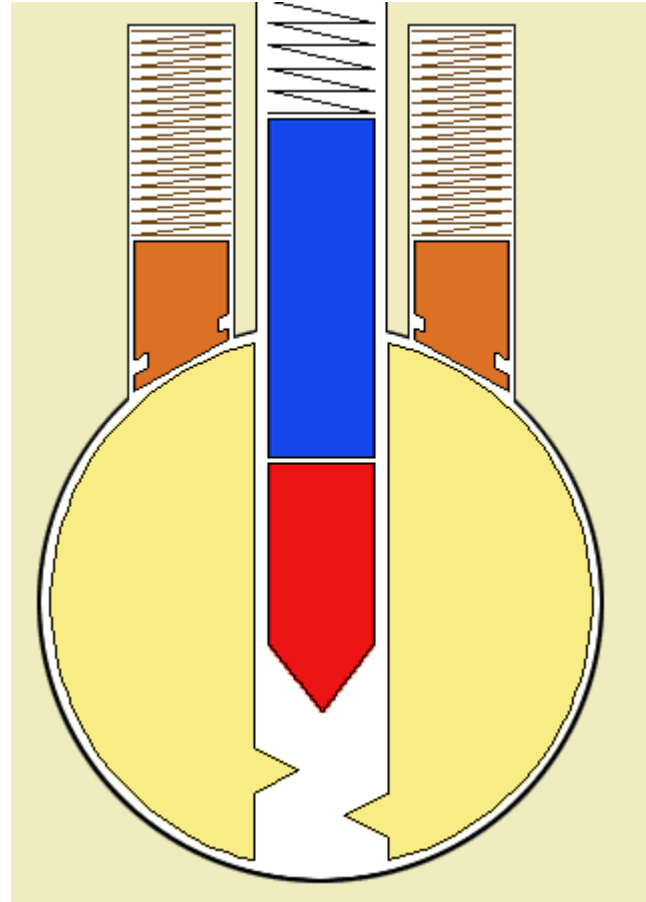
Trap Pins

Normal Key Operation



Trap Pins

Attempt Without a Key



Trap Pins

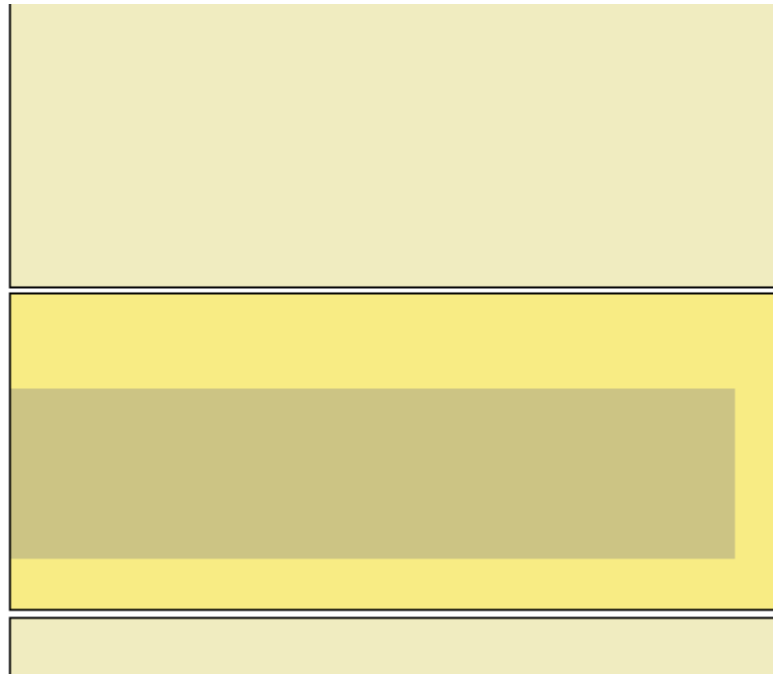
A Double-Edged Sword

- Absolute evidence of any any attempted pick or bypass
- Only one course of action after trap pins have fired
- Remove lock from door and replace with a new one
- Shallow drilling is simpler and offers more elegant protection...



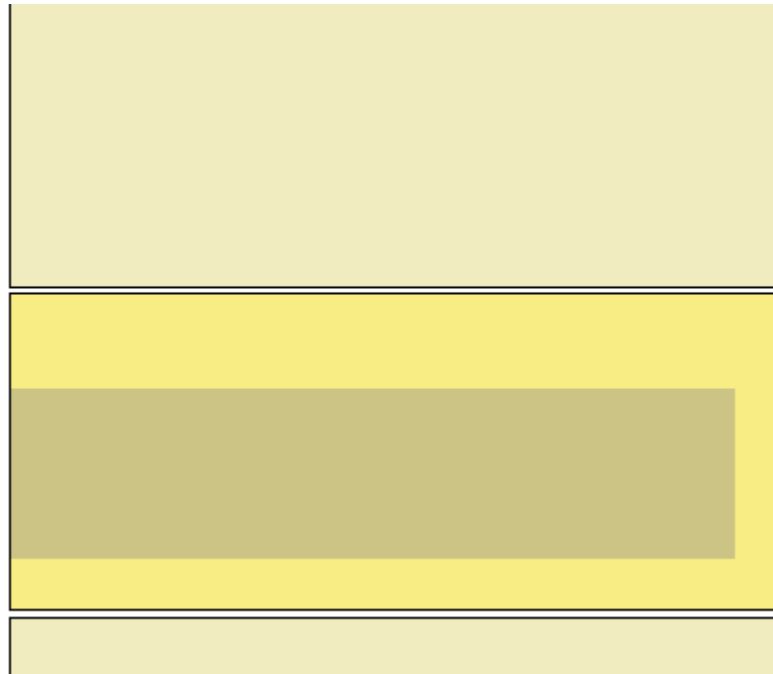
Shallow Drilling

Normal pin stack chambers being drilled...



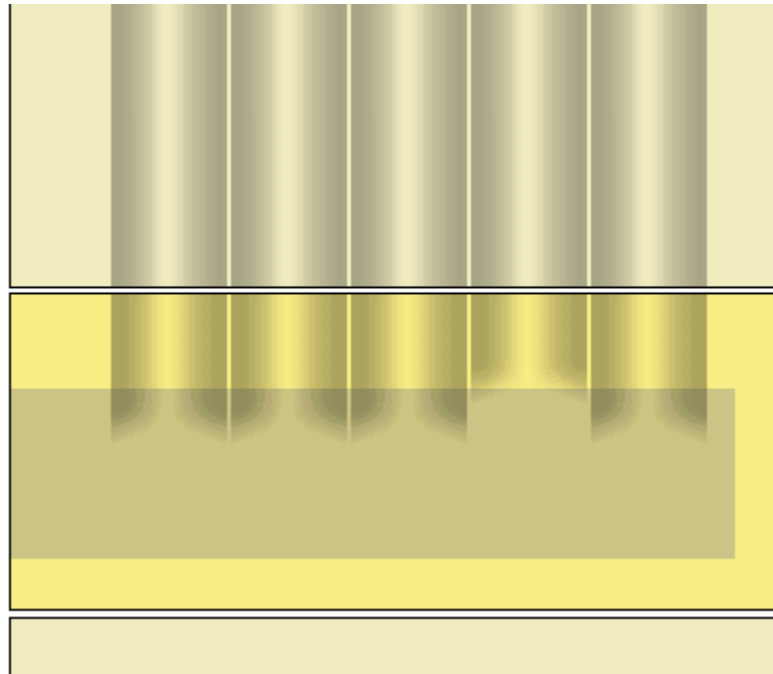
Shallow Drilling

Notice the difference with shallow drilling...



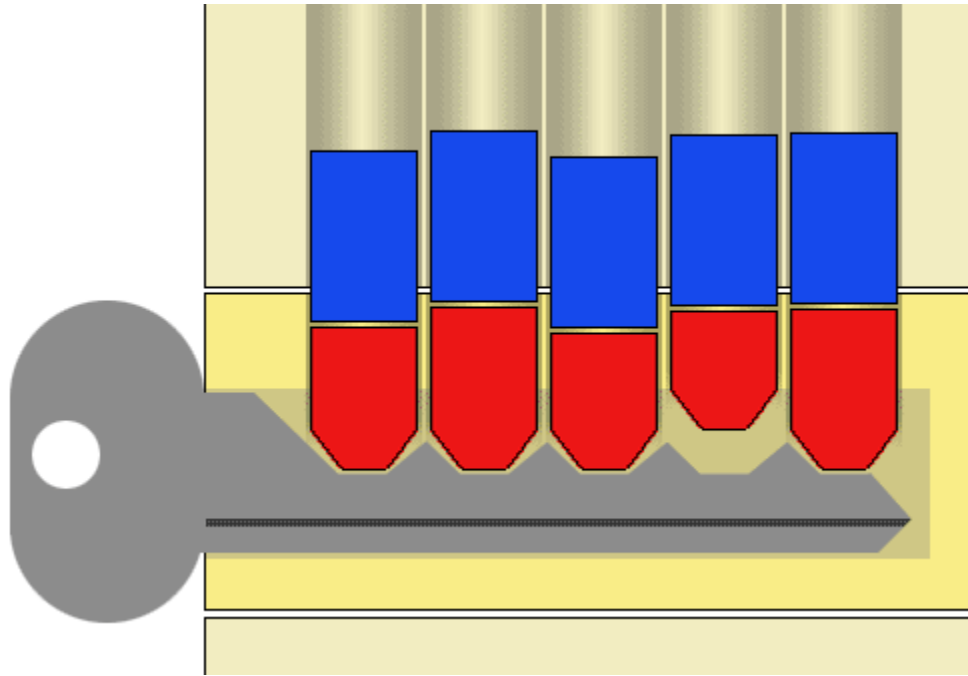
Shallow Drilling

Pin stacks have differing heights in their default position



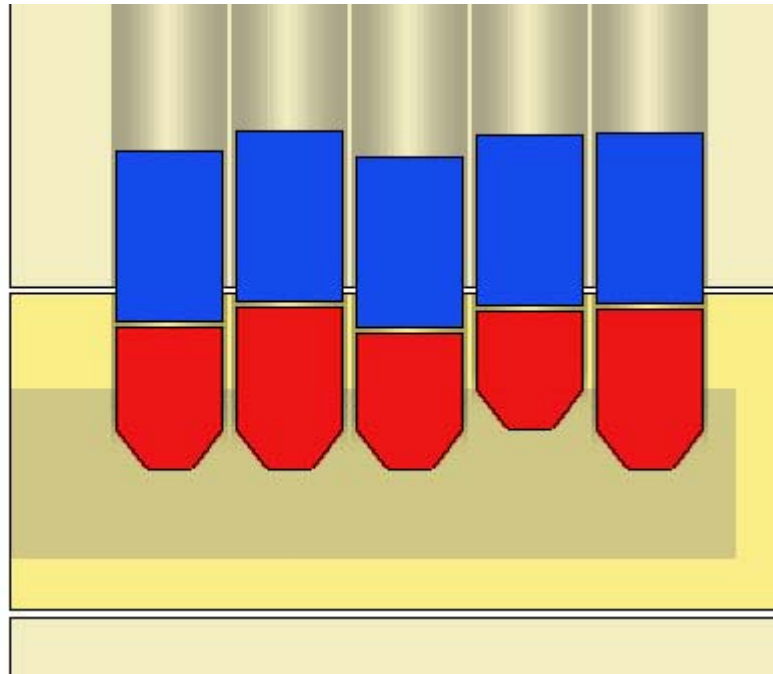
Shallow Drilling

Attempts at bumping will fail, not all pins touch the key



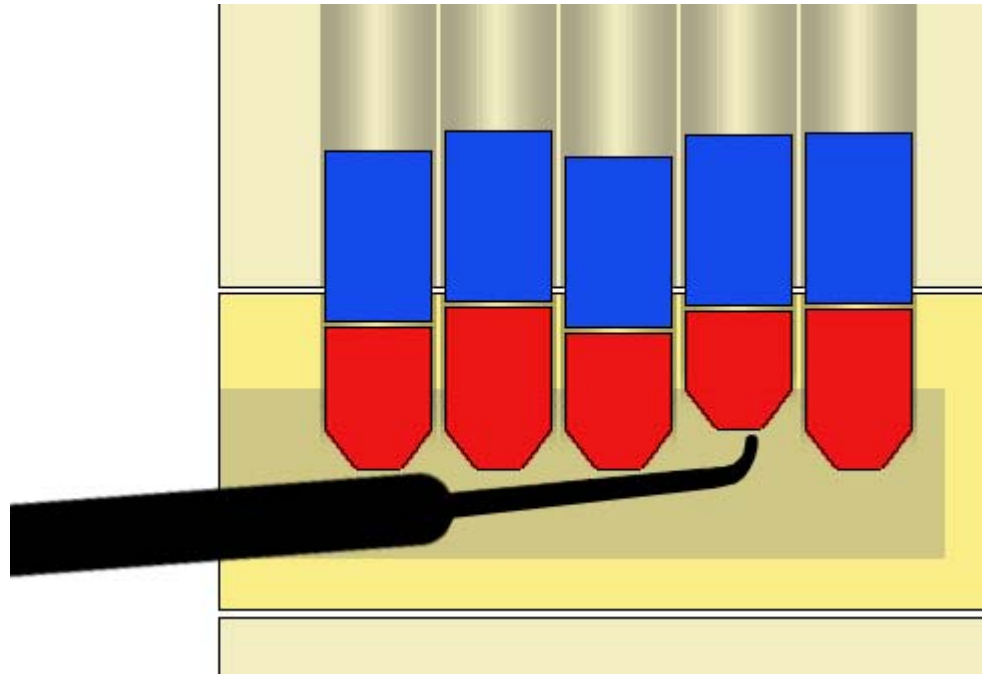
Shallow Drilling

No easy, outward evidence of this protection



Shallow Drilling

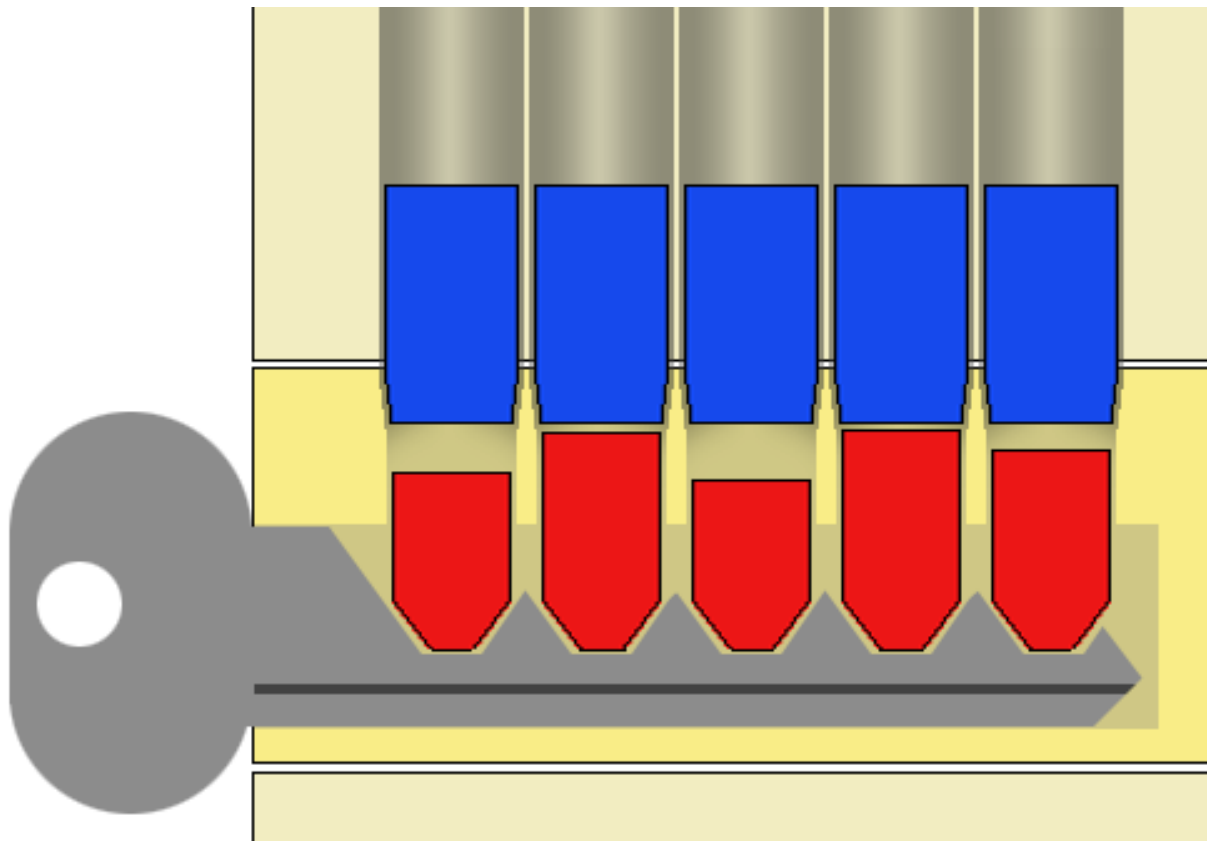
Conceivably possible to examine for shallow stacks...



... but what then, carry a whole ring of bump keys?

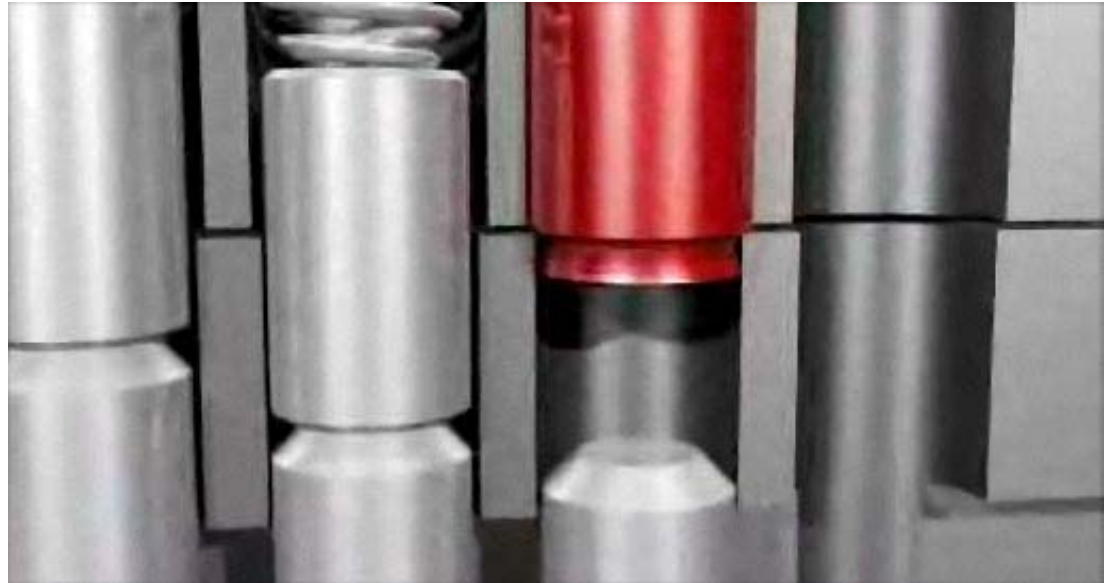
Top gapping

This design offers the most promise for fully hardening basic pin tumbler locks against the bump key attack.



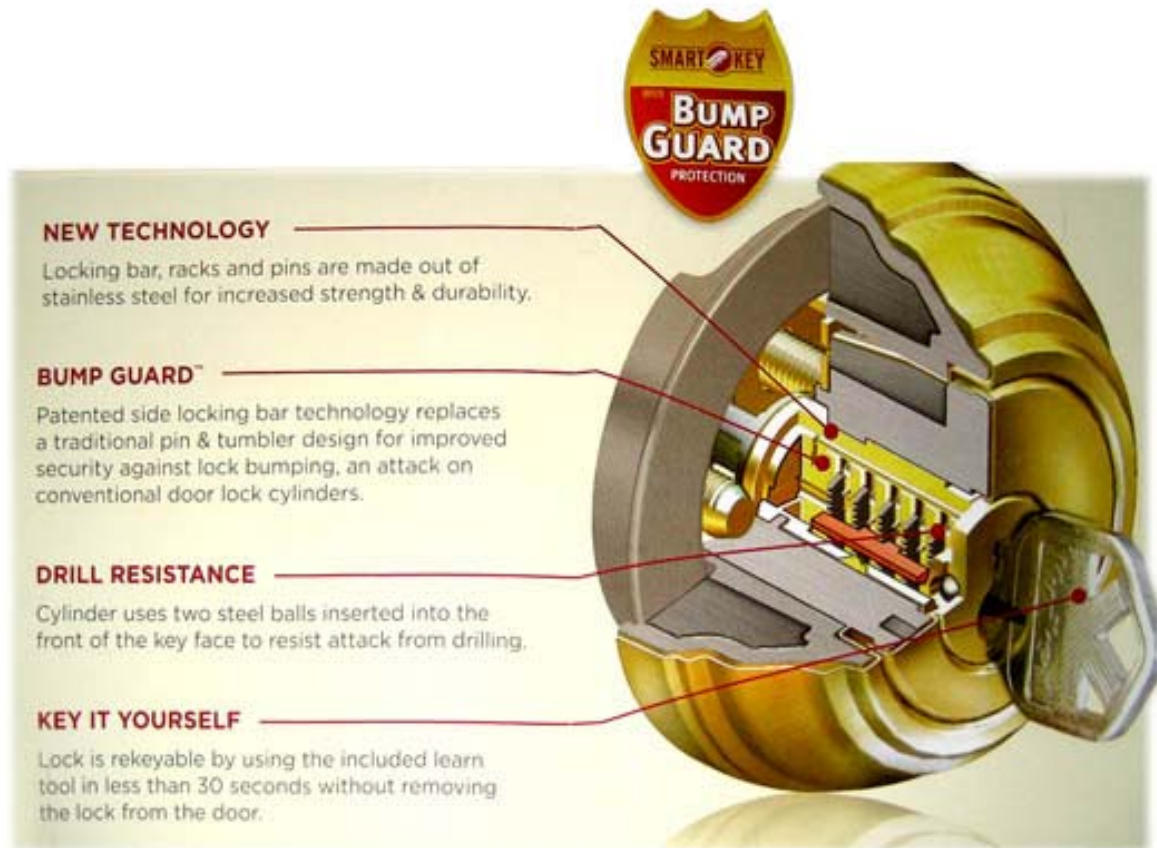
Top gapping

Master Lock has published on this topic and begun equipping locks with specialized top pins. Look for part numbers ending with the letter “N” or ask a locksmith.



Kwikset??

When even *this* company is making locks designed to prevent bump keying, it's finally gotten proper attention



What locks have these countermeasures?



- **Trap Pins**
 - M&C (Mitchel & Collin) "Antiklop" model
- **Shallow Drilling**
 - CES (Carl Eduard Schulte) VA5 & VB7 models
- **Top Gapping**
 - Master Lock / American Lock (retail or re-pinned)
- **Kwikset**
 - "Smart Series" line includes biometric options

Fluids & Gels

- **Pickbuster**
 - Invented by Mark Garratt
 - Distributed by *Almore* based in Pontypridd, Wales
- **Impedes Pin Movement**
- **Mixed Industry Reaction**
 - Pros: inexpensive, simple, bump resistant
 - Cons: not permanent, not perfect, and...
 - Significant concern about fouling
- **Weigh Costs and Benefits Yourself**



9. Large facilities have their own unique set of pitfalls and concerns

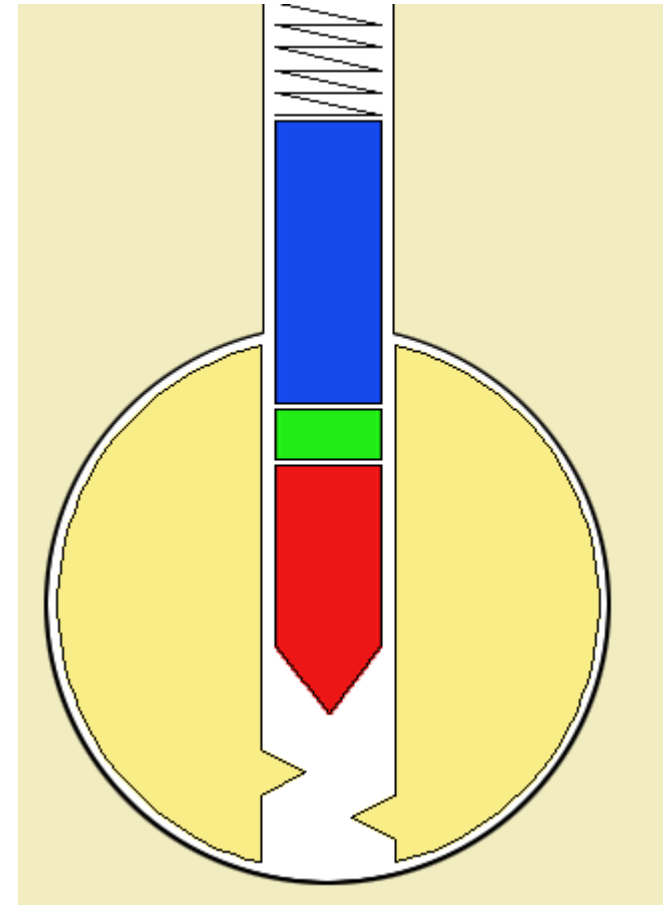
- Master keying
- Interchangeable cores
- Key control



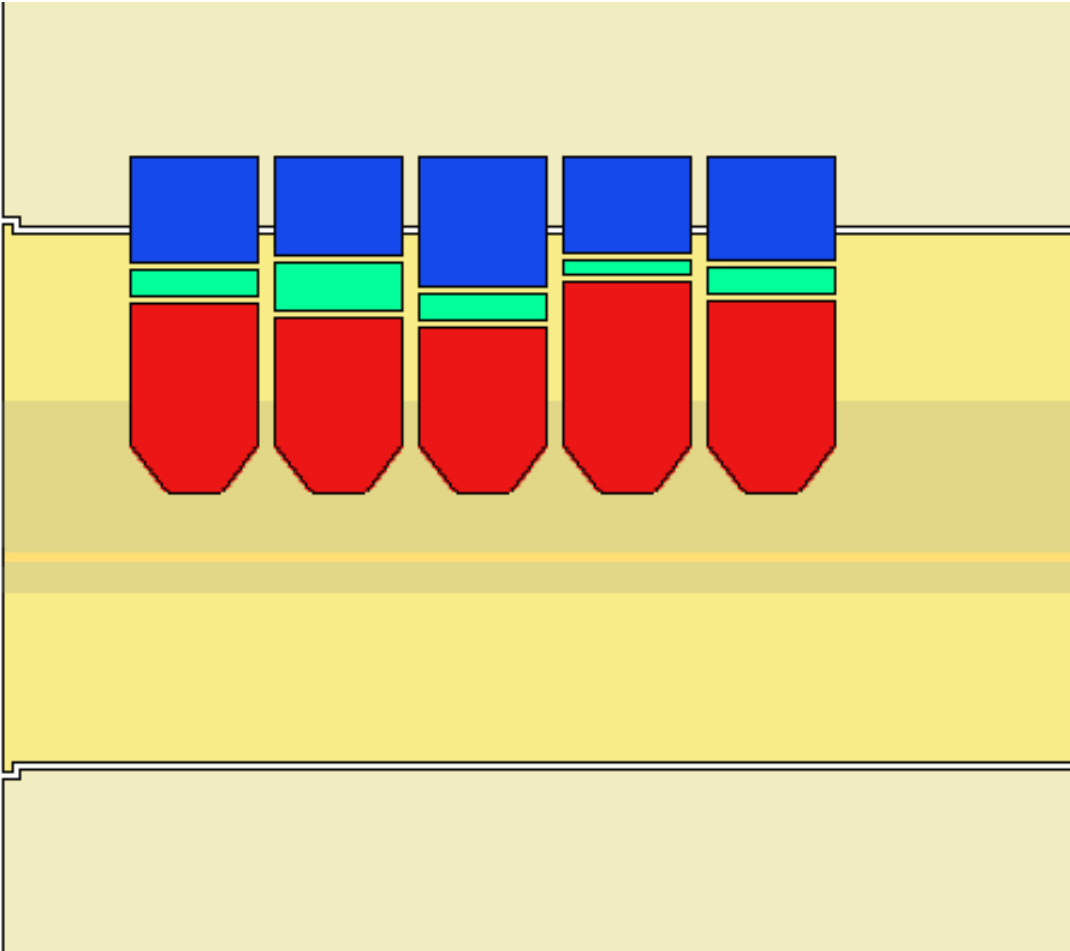
48:00

Master Key Theory

- Remember standard pin tumbler stacks?
- Same operation, with extra pin (or “wafer”) in the middle
- Potential for varied levels of clearance
- Also potential for many additional shear lines

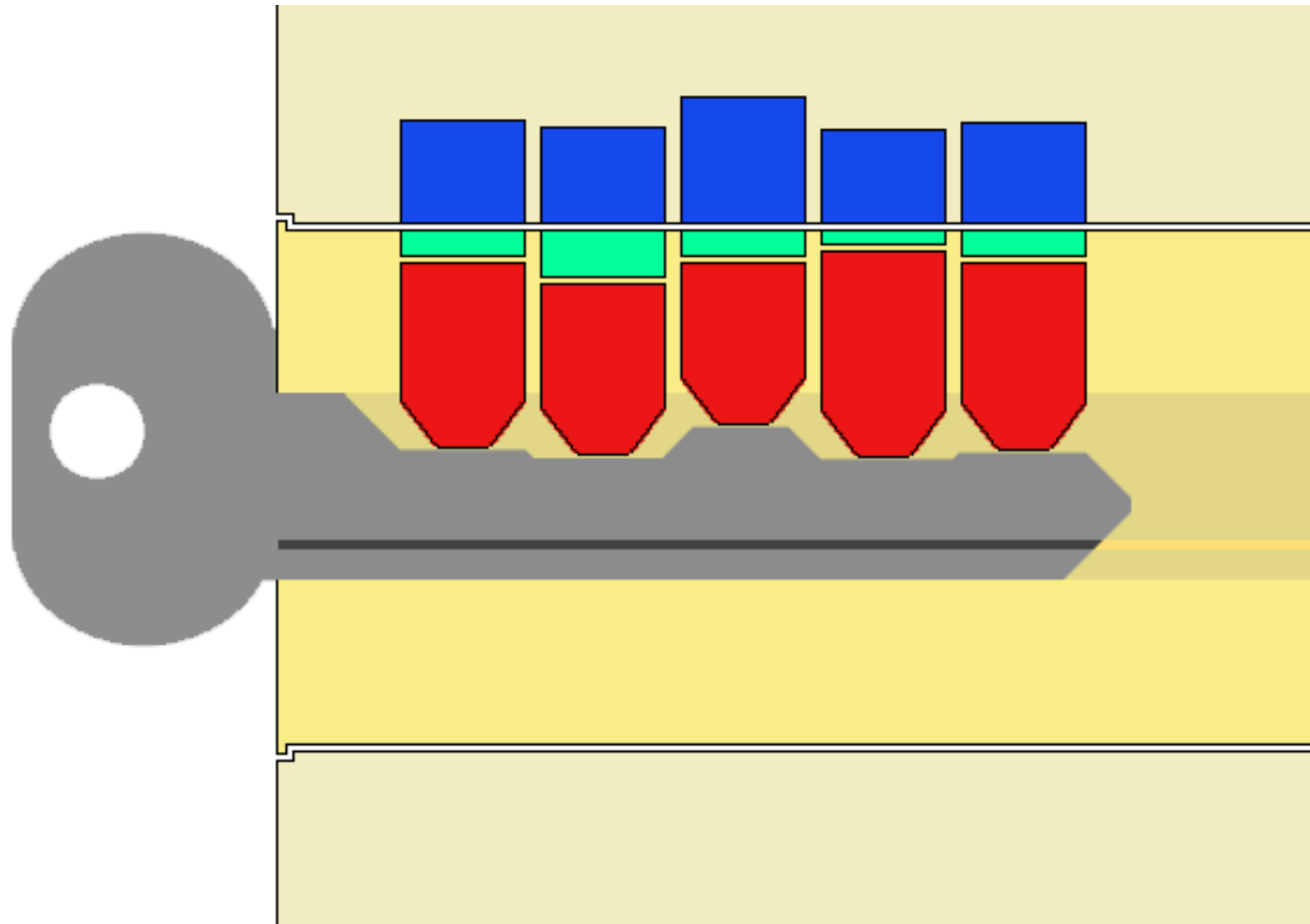


Master Pinning



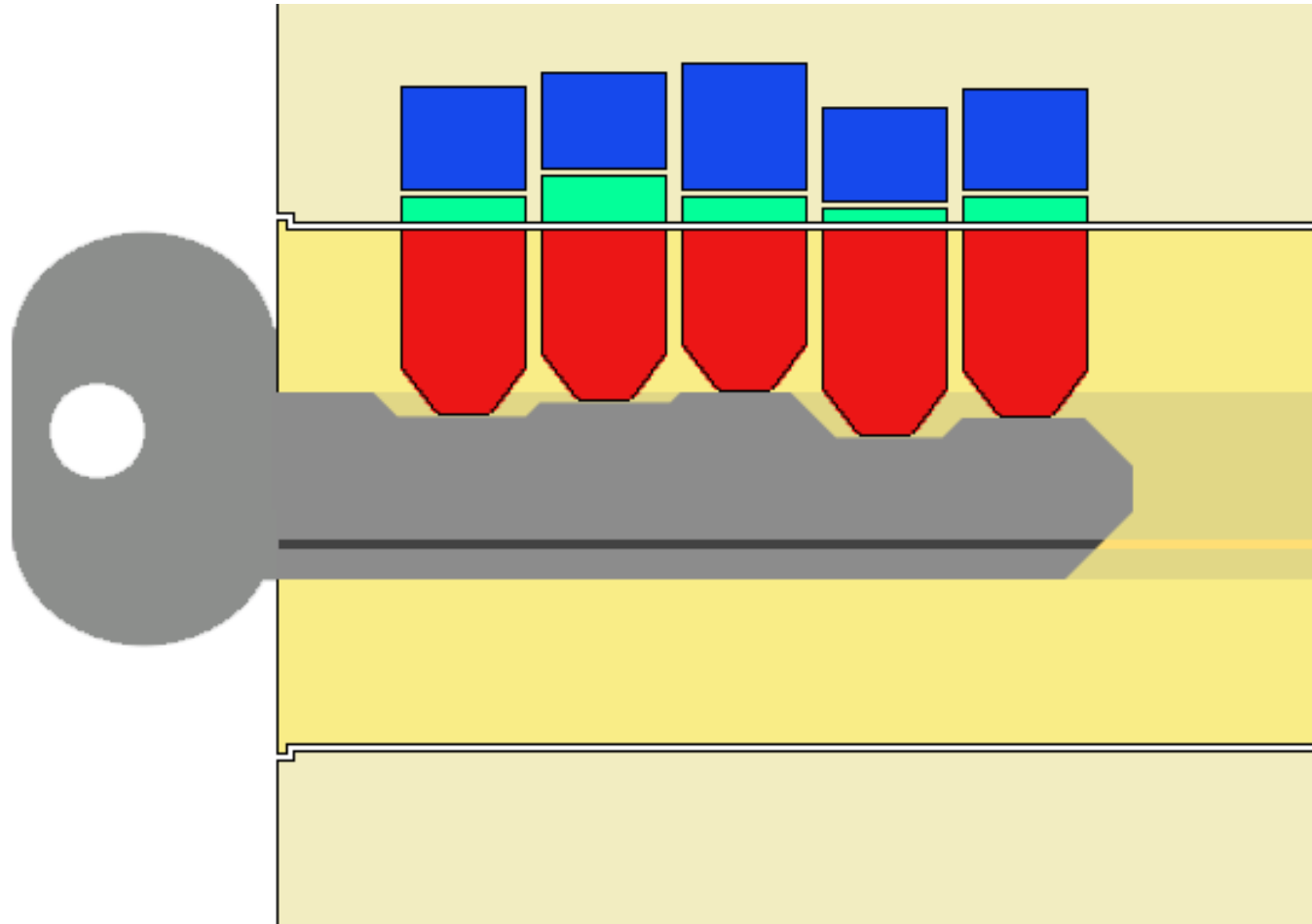
Master Pinning

User's "Change" Key



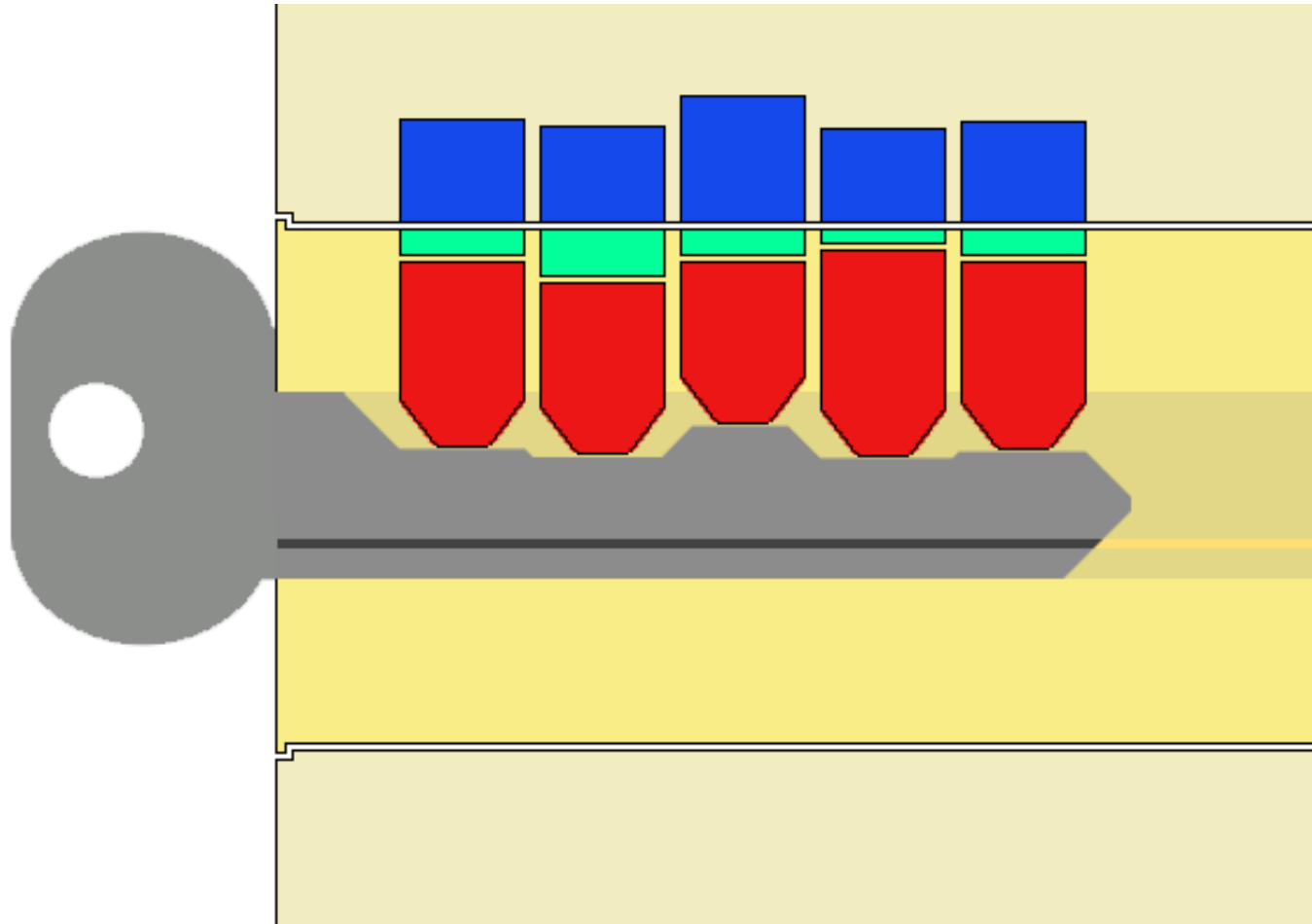
Master Pinning

Top Master Key



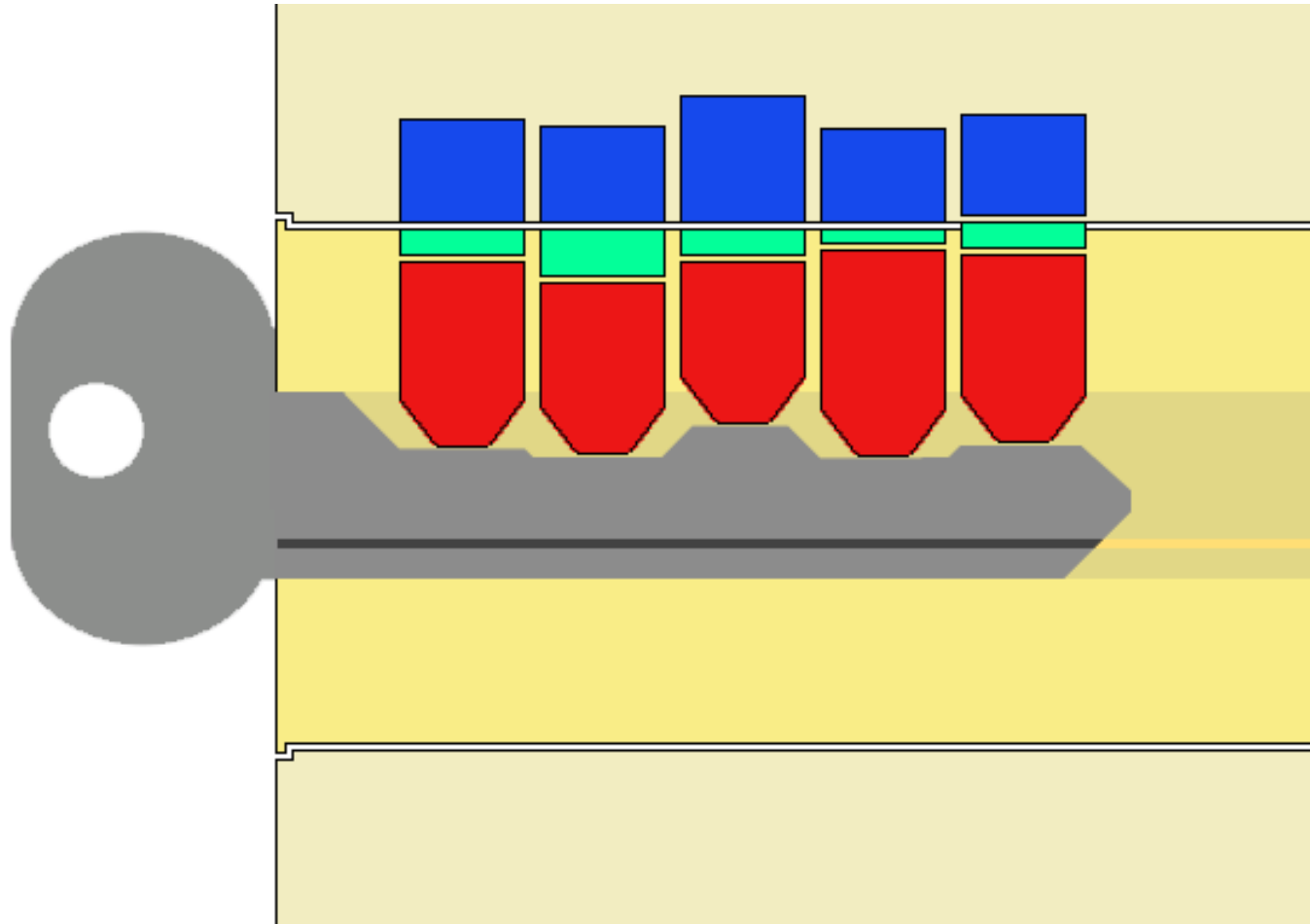
Master Pinning

Imagine a crafty user...



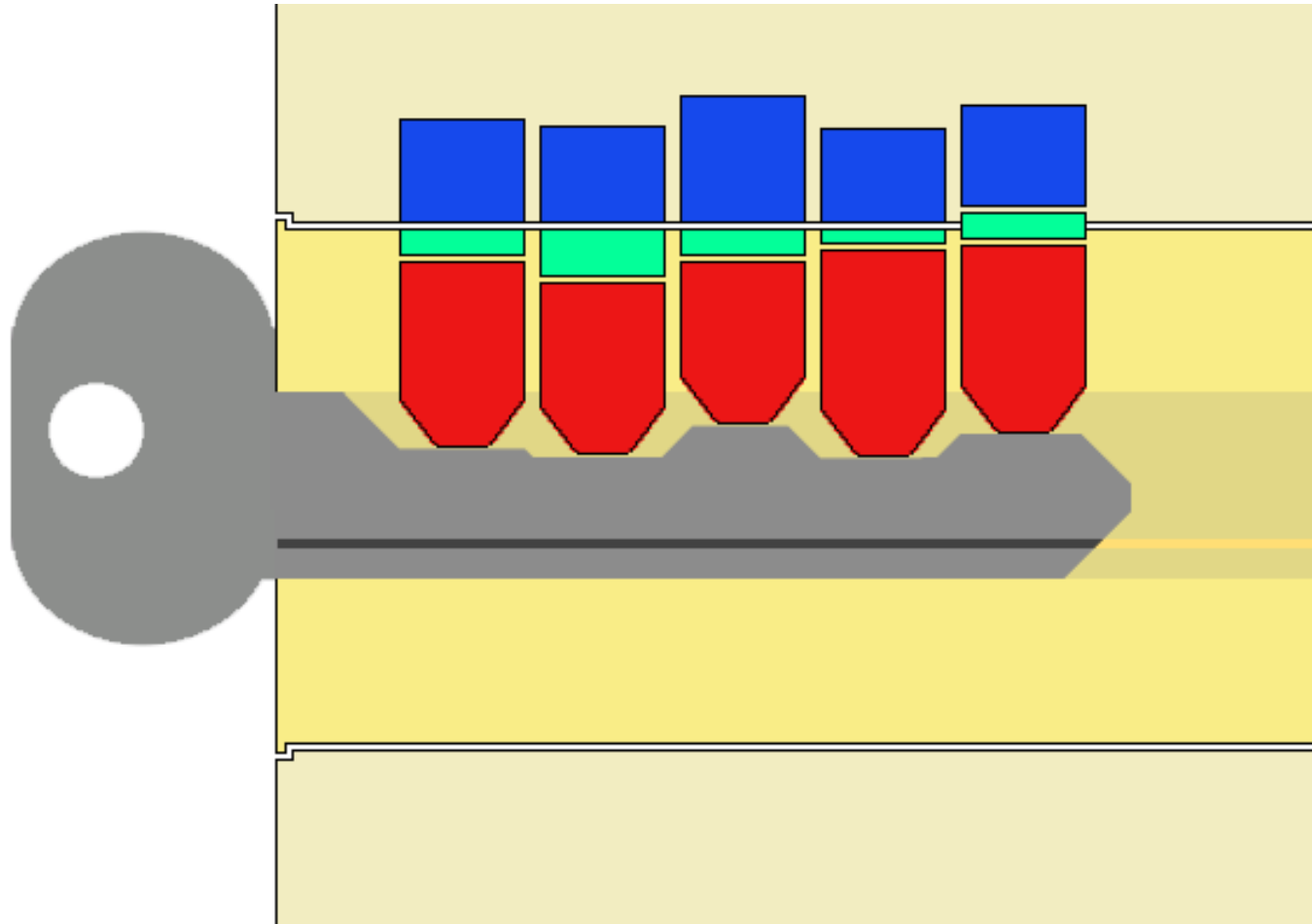
Master Pinning

They modify their key... it doesn't open



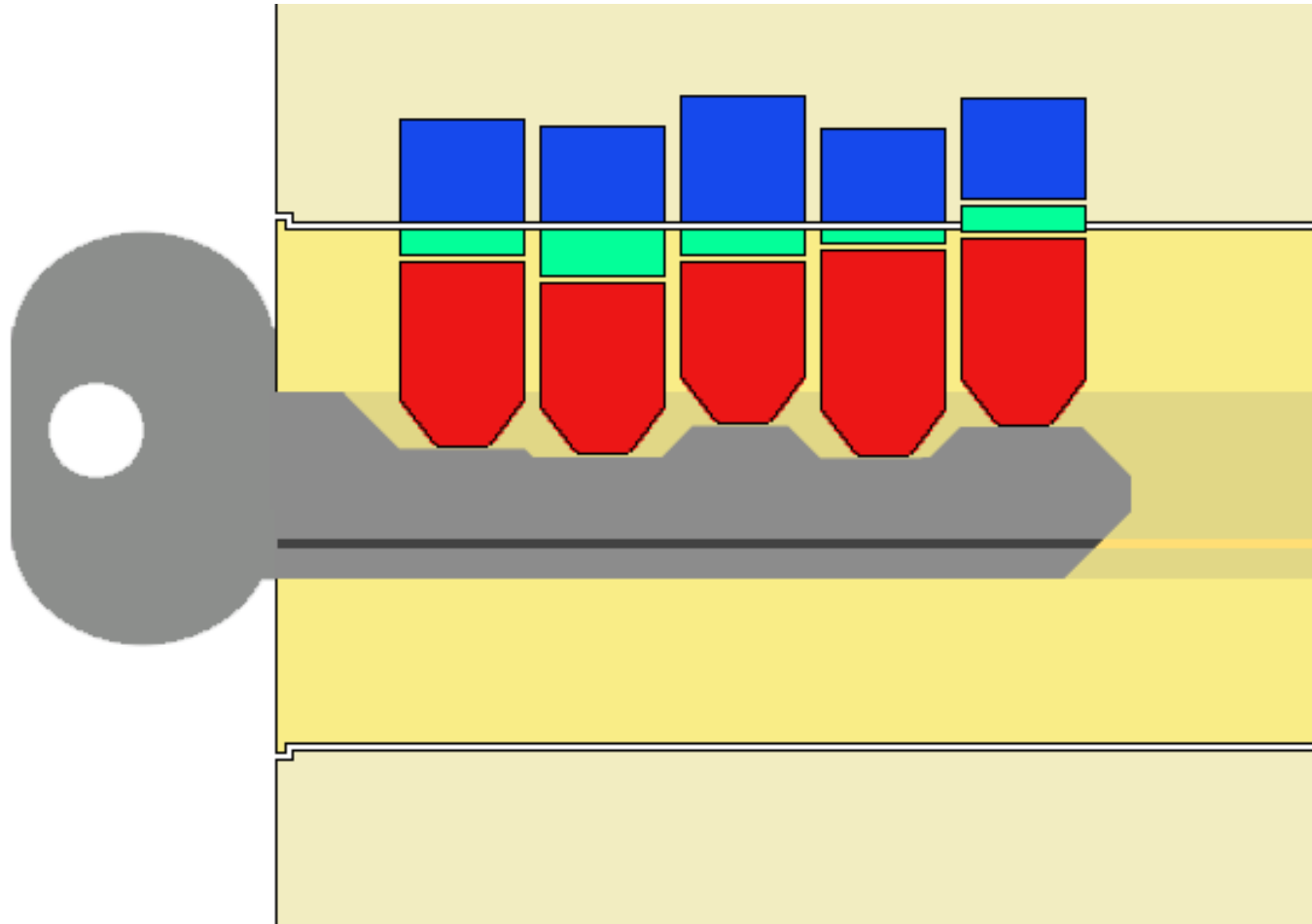
Master Pinning

They modify their key... it doesn't open



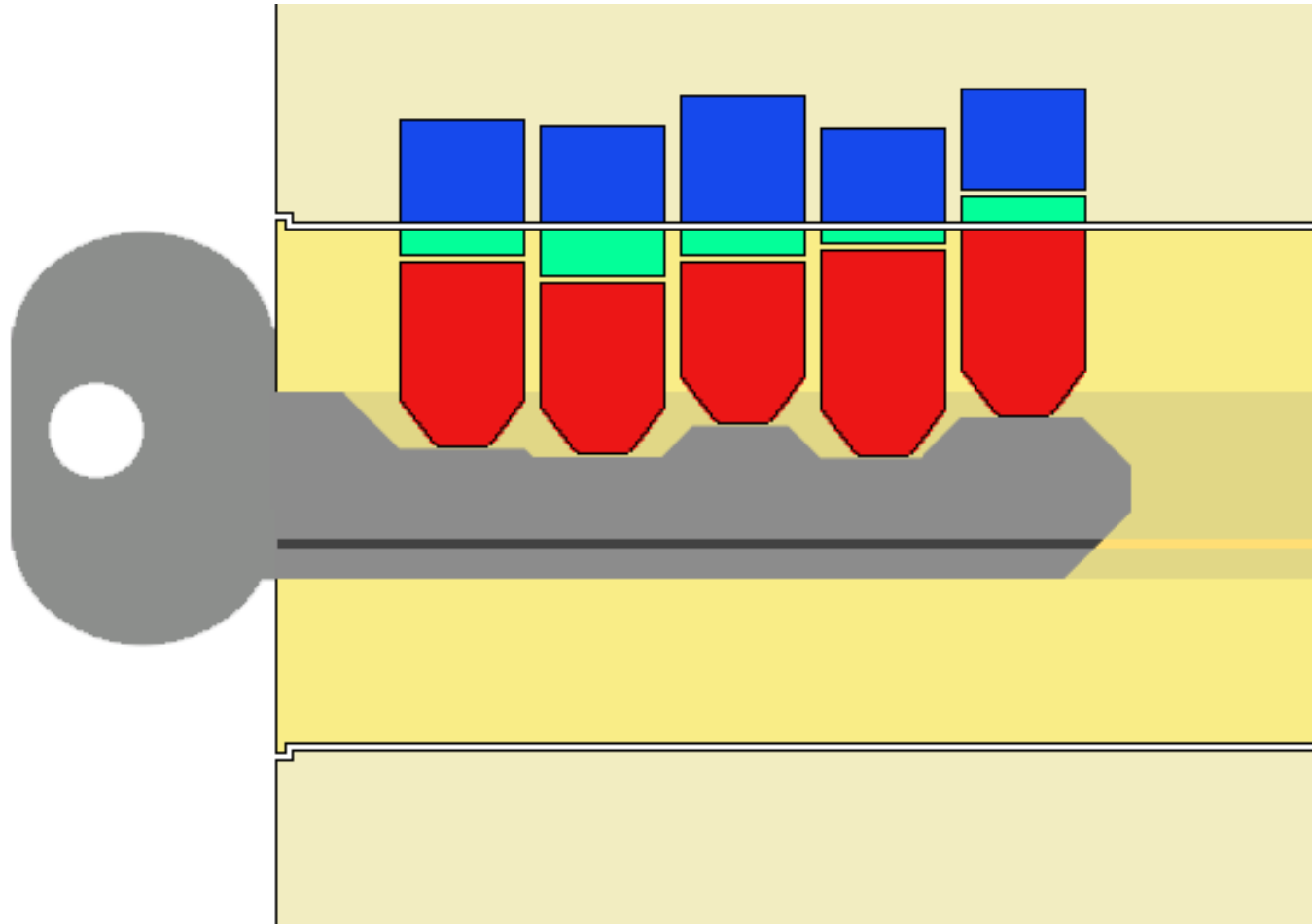
Master Pinning

They modify their key... it doesn't open



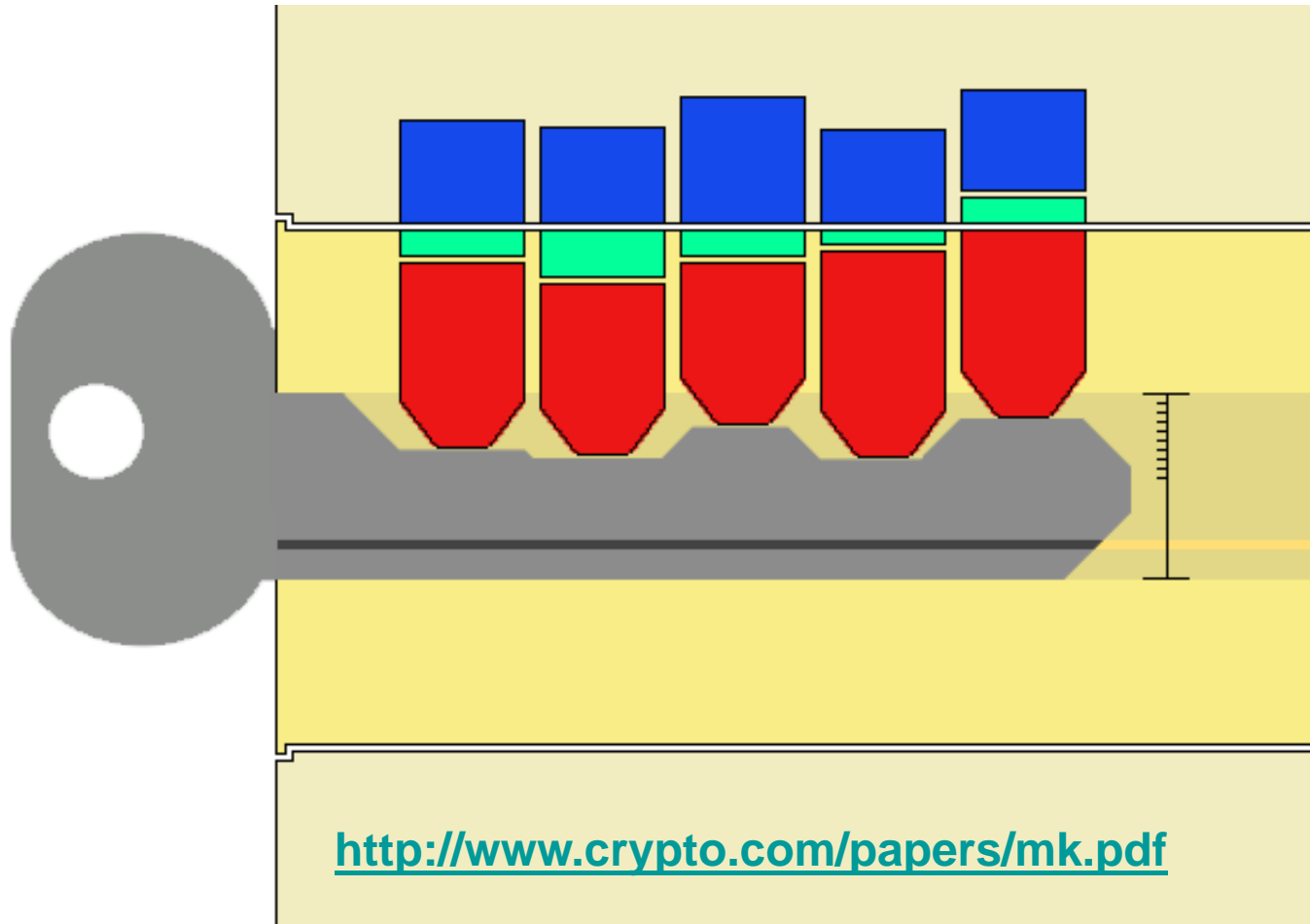
Master Pinning

They modify their key... suddenly it opens!



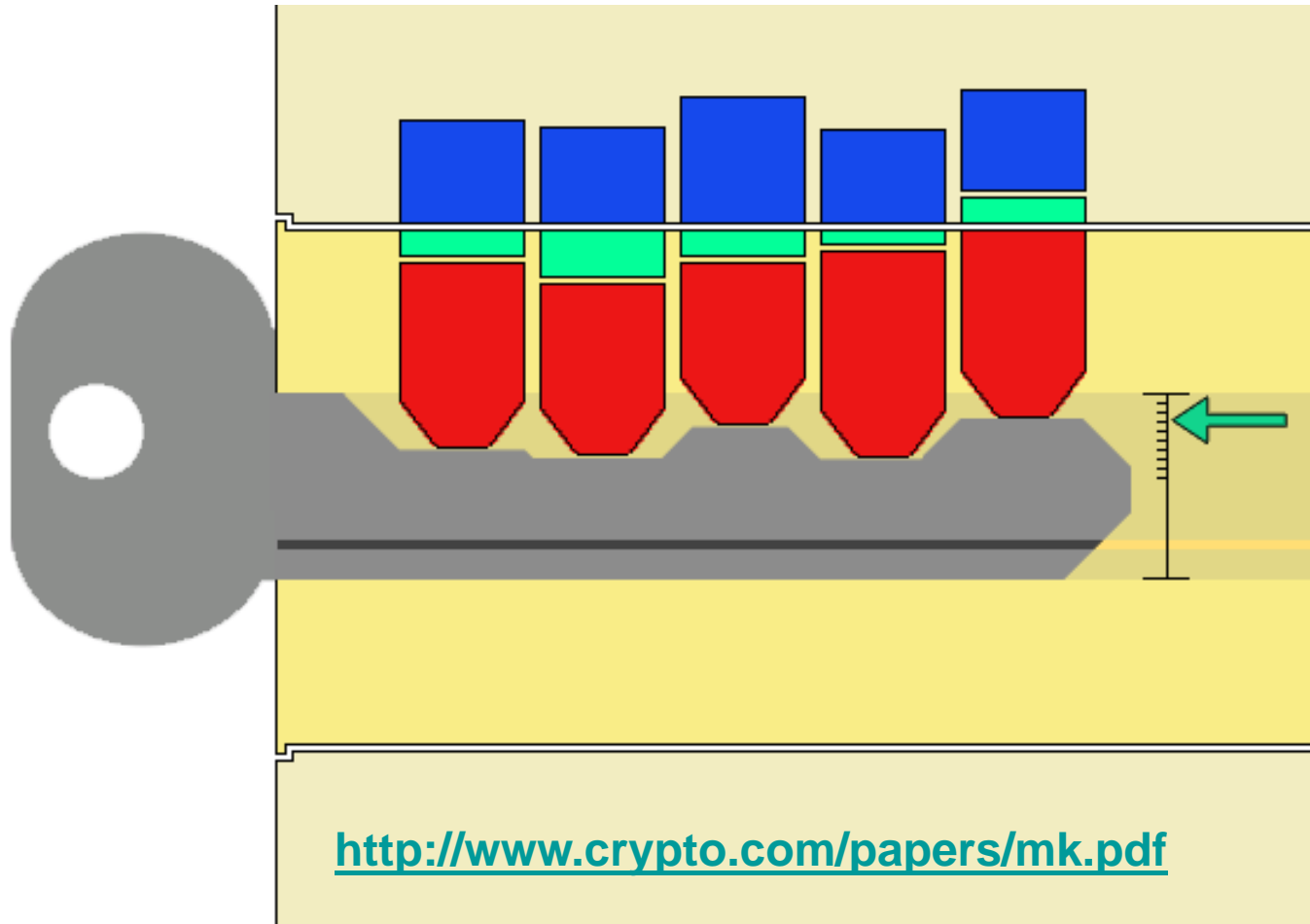
Master Pinning

This last chamber is now at the “master” height



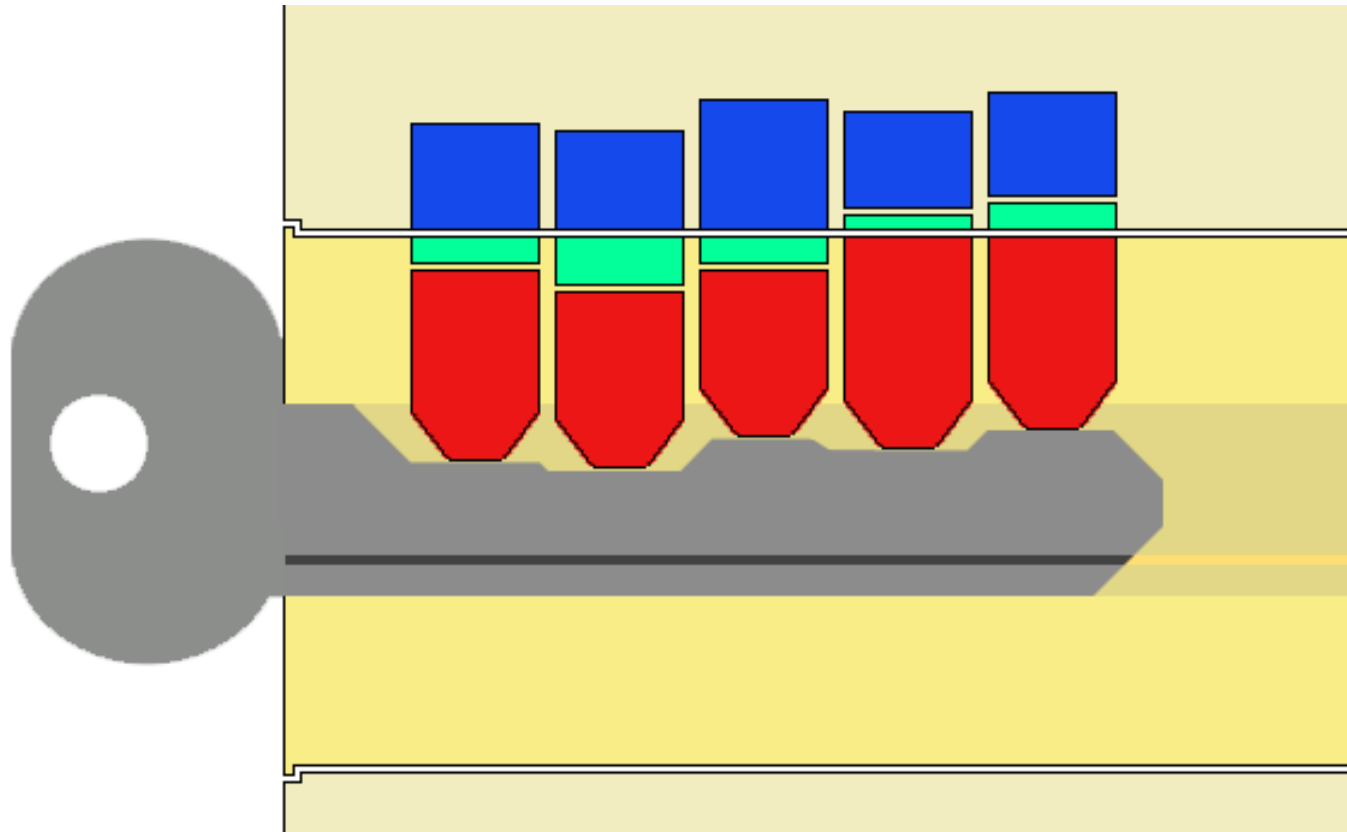
Master Pinning

This bitting can be measured



Master Pinning

This is how “intermediate master” keying works



Keep in mind... in a large, mastered facility *all* doors have within them the full top master pinning. Compromise of any single door can give access everywhere.

SFIC Locks

- **Small Format Interchangeable Core**

- BEST
- Yale
- Others

- **Easy to Manage**

- Plug and pins all eject as a single, contained unit

- **Hard to Pick**

- Multiple independent shear lines
- Keyways are worse than any nightmares you could find at the bottom of a bottle or at the hands of the U.S. Congress



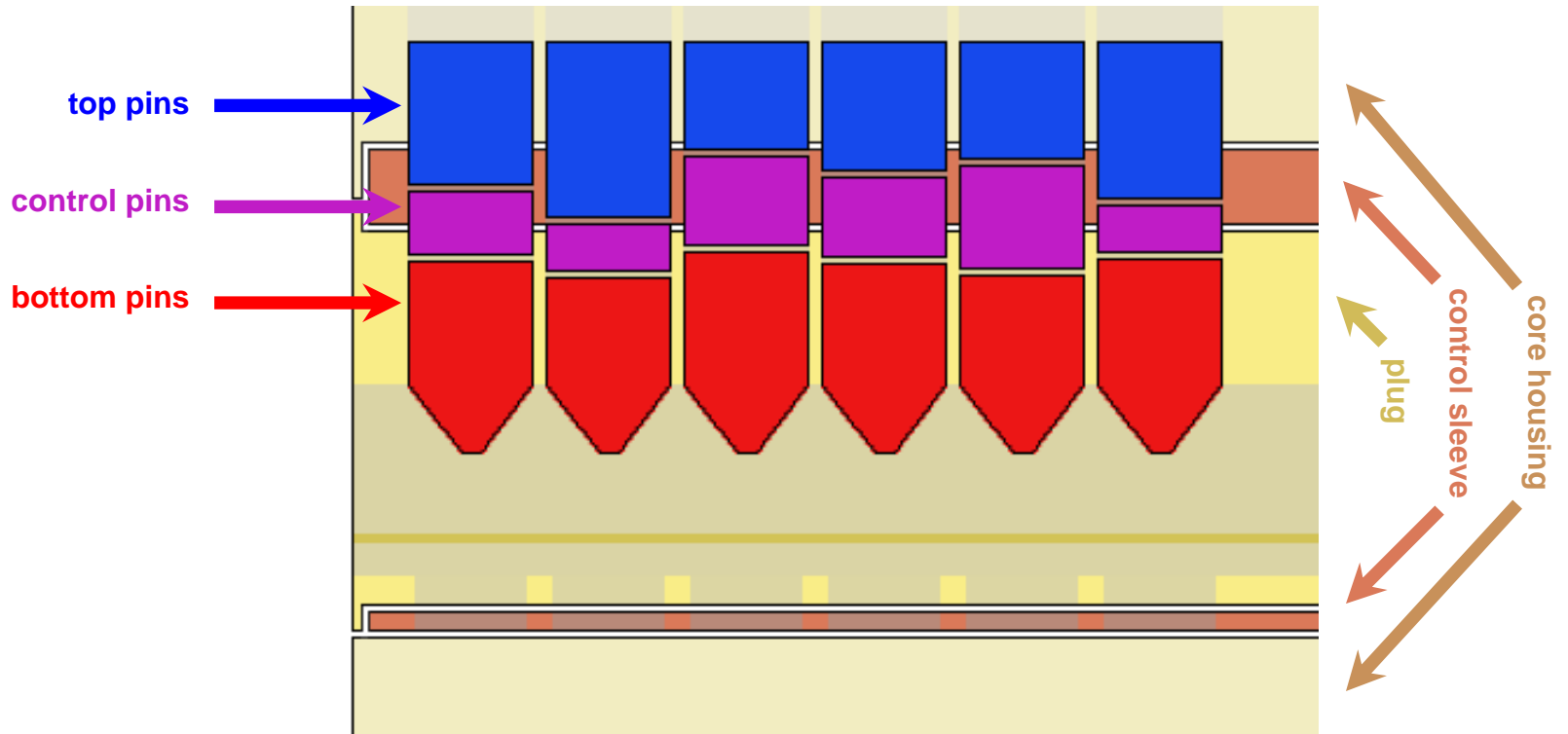
SFIC Locks

- **Very popular in large institutions**
- **Cores remove with a “control key”**
- **Two independent shear lines**
 - Raising pins to one level allows plug to rotate freely
 - Raising pins to other shear line locks plug and control sleeve together and they turn as one, either exposing or retracting core’s retaining tab
- **Picking attempts typically fail with standard tools**
 - Tension binds across both shear lines



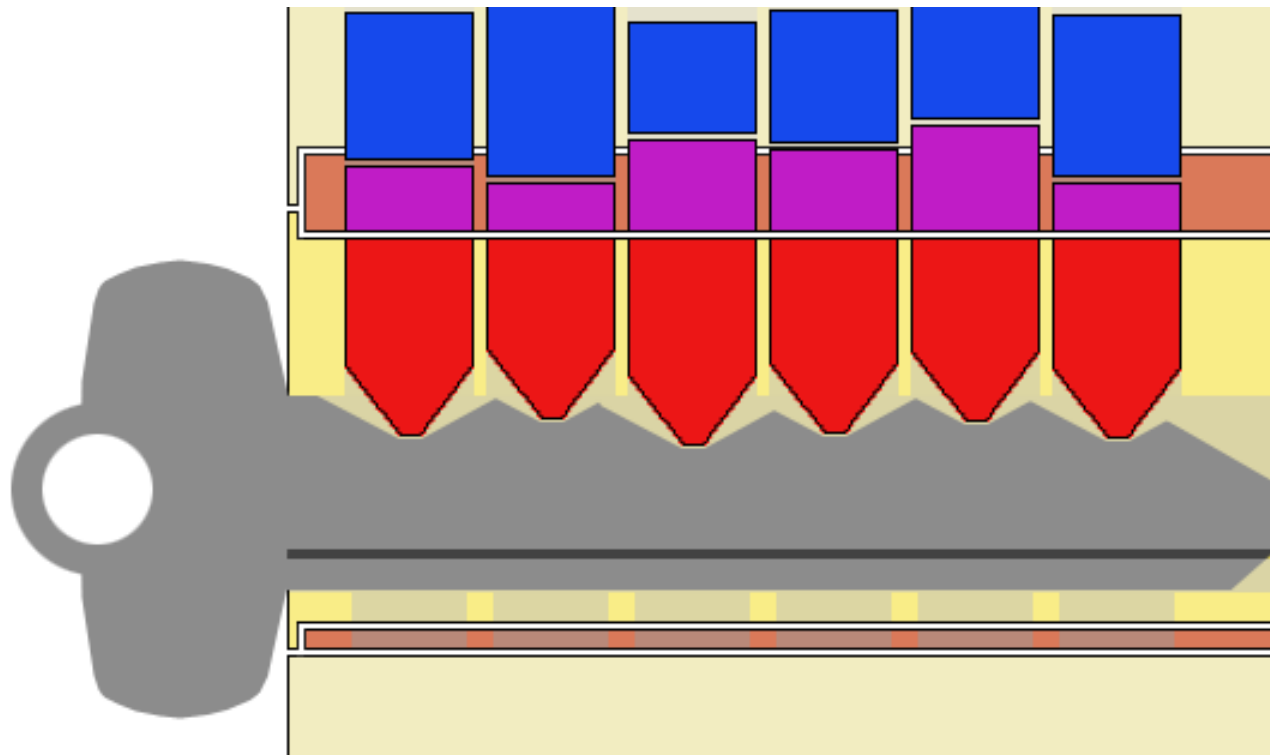
SFIC Locks

Pin Stacks



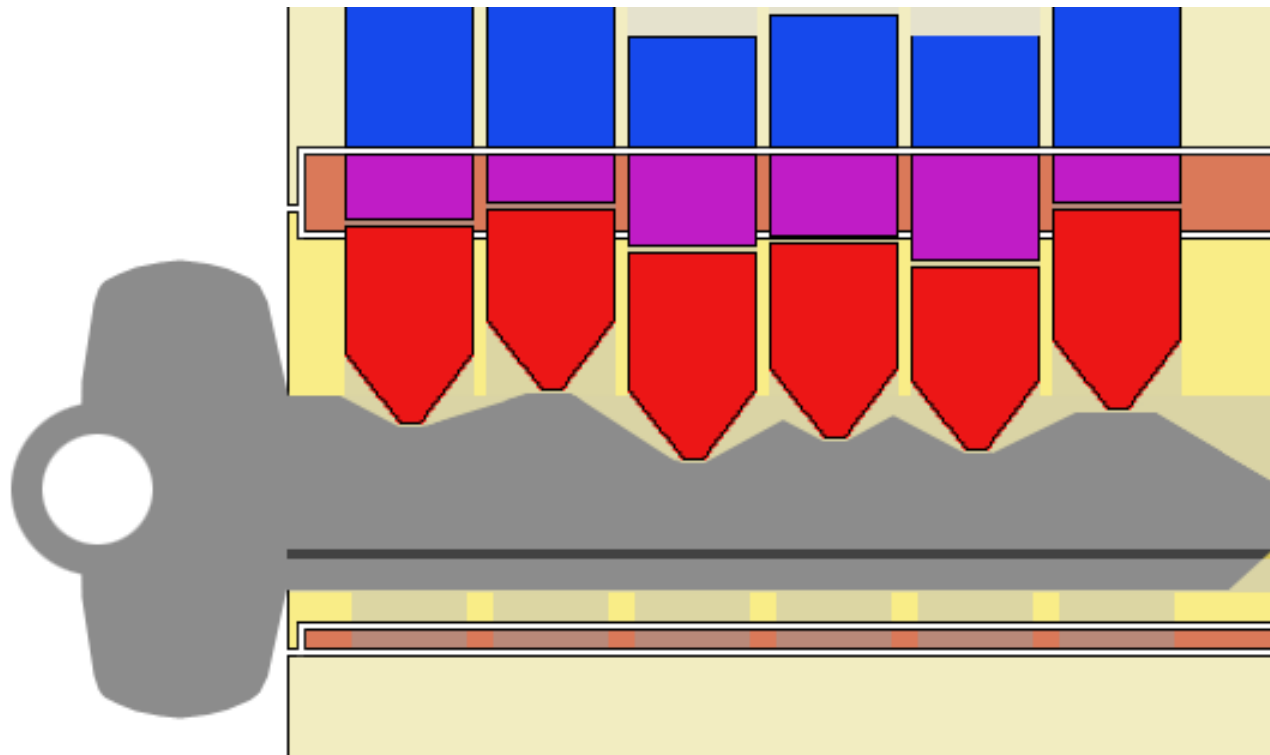
SFIC Locks

Operating Key



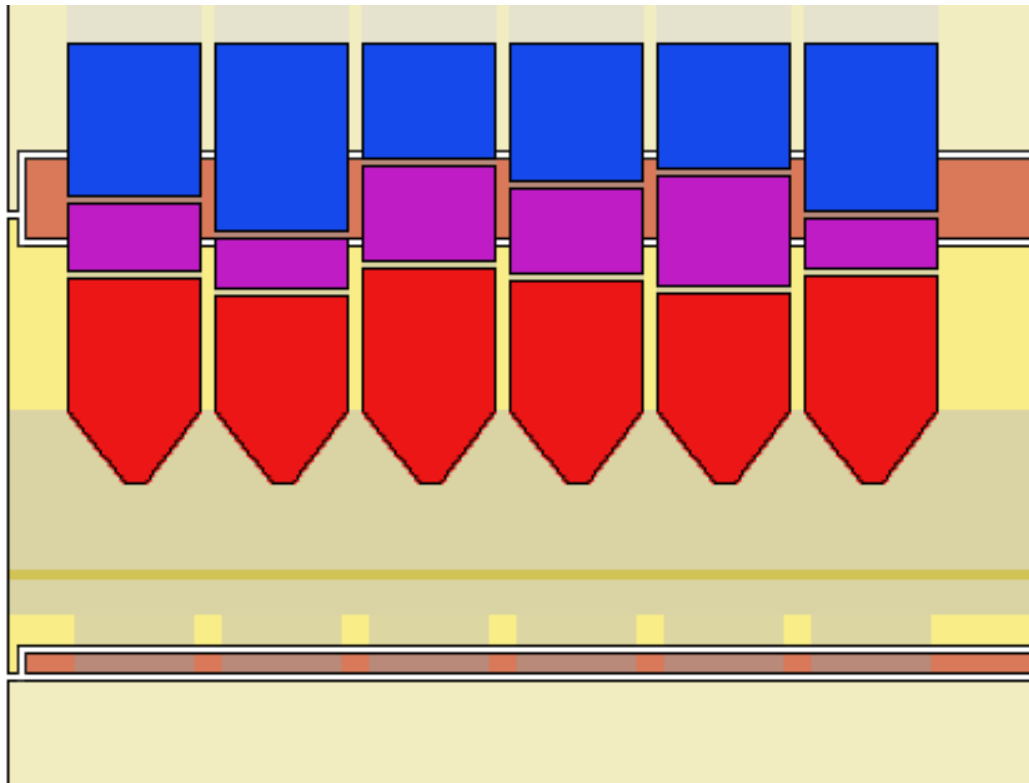
SFIC Locks

Control Key



SFIC Locks

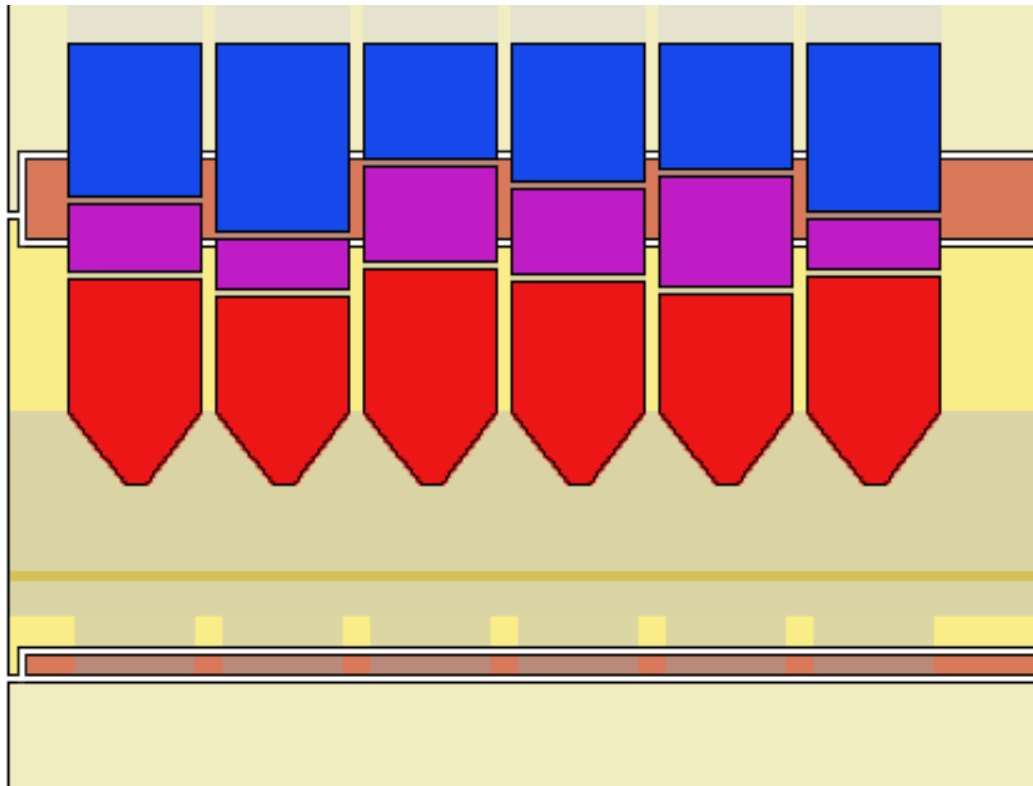
- **Normal picking attempts typically fail**
 - Tension binds across both shear lines
 - Extremely likely to set pins in various places



SFIC Locks

- **There are specialized tools**

- Torsion wrench with “fingers” puts pressure on only one shear line
- Still very difficult, however, due to tight tolerances and keyways



SFIC Locks

- **Matt Blaze's modified sleeve**
 - Nothing for specialized “finger wrench” to grab



SFIC Locks

- **New BEST design**

- I believe the locks are manufactured this way now



Key control

- Preventing illicit copies
- Using “restricted” keyways
- Inability to make blanks
- E-Z Entrie vs. Side Cuts



10. Security in the Real World

- **Technical Finesse or Brute Force**

- Common criminals do not pick locks
- A \$100 lock in a \$10 door is little help

- **Doors**

- Solid-core, heavy material
- Heavy hinges, screws deep into frame
- Deadbolts with round core(s)

- **Windows**

- Break glass to reach knobs
- Shatterproof film

- **Visibility**

- Motion-sensing lights
- Keep bushes & trees trimmed



So what is a “good” lock?

- **Manufacturers whom I love...**

- **SCORPION** (slider-based sidebar)
- **EVVA** (sliders & sidebars)
- **SCHLAGE Primus** (unique sidebar system)
- **BEST** (SFICs)
- **ABUS** (Granit & Diskus)
- **ABLOY** (rotating disk)
- **AMERICAN** (shackle-less padlock)
- **TrioVing** (double mushroom pins)
- **KARAMAS** (X-07 and X-09 dials)
- **SG SARGENT AND GREENLEAF** (armory locks, combo locks, safes, deposit boxes)



- **Good rules of thumb**

- You get what you pay for
- Keep the big picture in mind
- Keep tinkering and questioning

Security is only as effective...



... as the person using it

A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores



A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle



A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle
- **Peterson Bypass Tool**
 - Slips all the way through core
 - Interacts with control cylinder directly



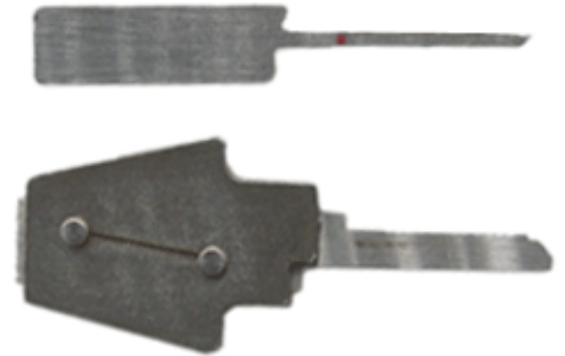
A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle
- **Peterson Bypass Tool**
 - Slips all the way through core
 - Interacts with control cylinder directly
- **Security Wafer**



A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle
- **Peterson Bypass Tool**
 - Slips all the way through core
 - Interacts with control cylinder directly
- **Security Wafer**
- **Wafer Breaker Tools**



A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle
- **Peterson Bypass Tool**
 - Slips all the way through core
 - Interacts with control cylinder directly
- **Security Wafer**
- **Wafer Breaker Tools**









A Security Fable

- **American 700 Padlock**
 - Solid design
 - Serrated pins
 - Interchangeable cores
- **Core Operation**
 - Back of plug... half circle
 - Control cylinder... quarter circle
- **Peterson Bypass Tool**
 - Slips all the way through core
 - Interacts with control cylinder directly
- **Security Wafer**
- **Wafer Breaker Tools**
- **Shackless Padlock... the American 2000**



So what is a “good” lock?

● Manufacturers whom I love...

-  **SCORPION** (slider-based sidebar)
-  **EVVA** (sliders & sidebars)
-  **SCHLAGE Primus** (unique sidebar system)
- **BEST** (SFICs)
-  **ABUS** (Granit & Diskus)
-  **ABLOY** (rotating disk)
- **AMERICAN** (shackle-less padlock)
- **TrioVing** (double mushroom pins)
- **KARAMAS** (X-07 and X-09 dials)
-  **SARGENT AND GREENLEAF** (armory locks, combo locks, safes, deposit boxes)



● Good rules of thumb

- You get what you pay for
- Keep the big picture in mind
- Keep tinkering and questioning