Key Decoding and Duplication Attacks for the Schlage Primus High-Security Lock

David Lawrence Robert Johnson Gabriel Karpman

locks@mit.edu

DEF CON 21

August 3, 2013

Standard pin-tumbler locks

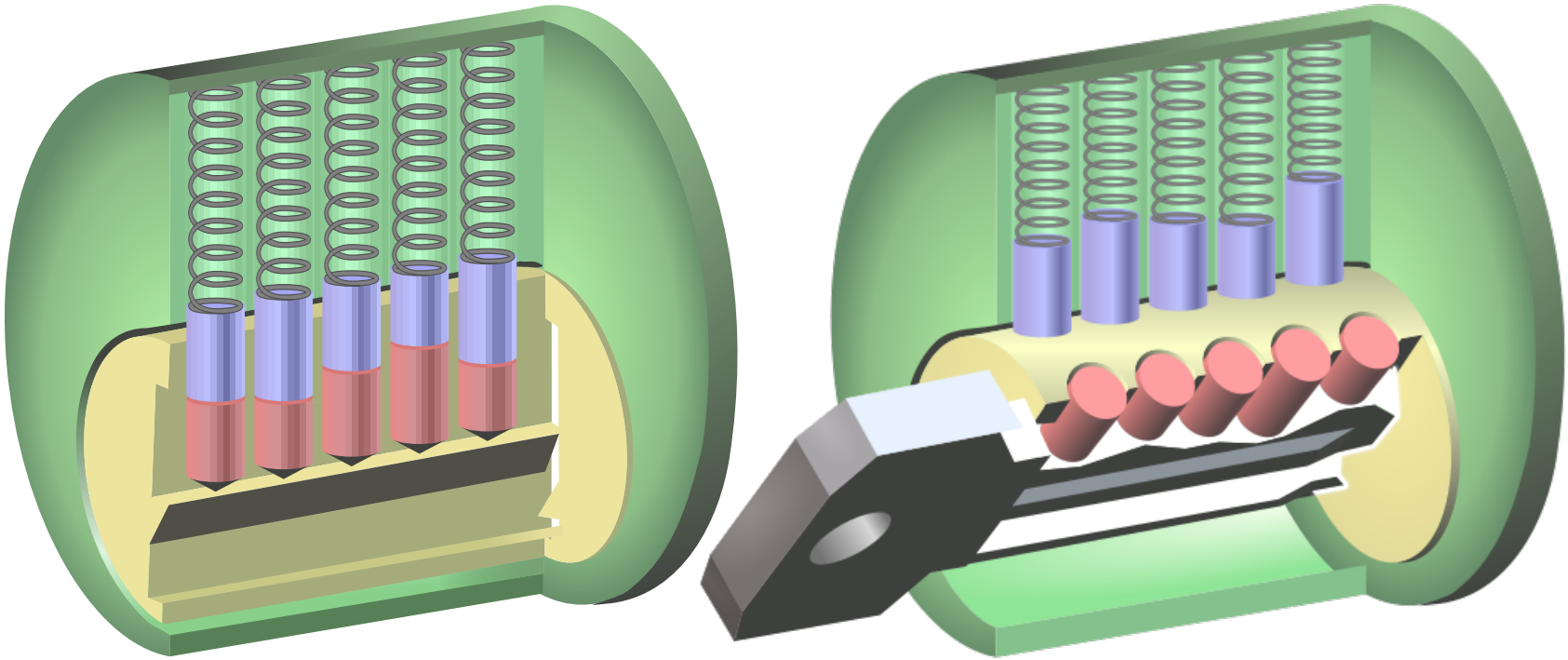


Photo credit: user pbroks13 on Wikimedia Commons. Licensed under GFDL or CC-BY-SA-3.0.

Vulnerabilities

1. **Key duplication**: get copies made in any hardware store.
2. **Manipulation**: susceptible to picking, impressioning, etc.

The Schlage Primus

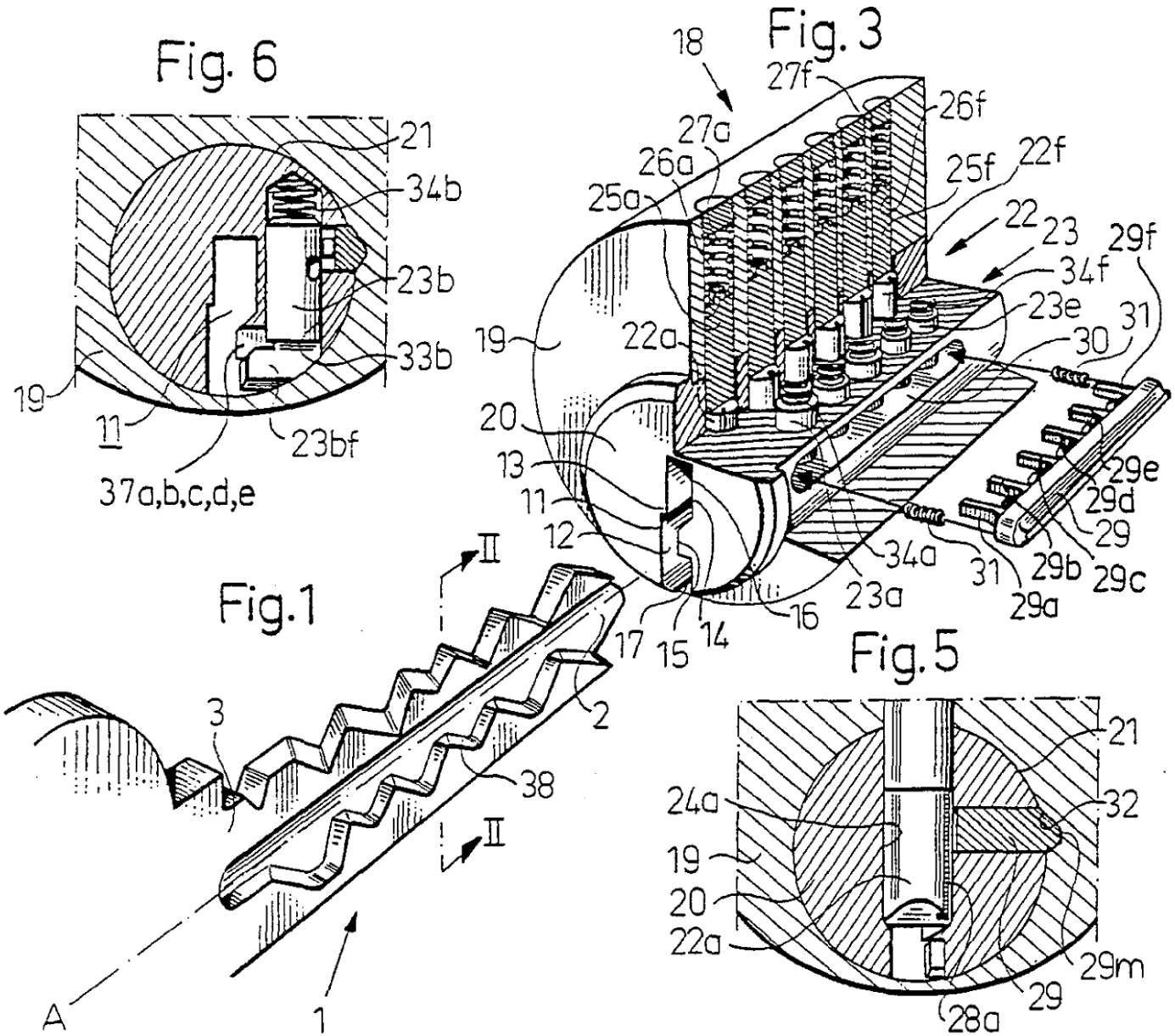
Based on a pin-tumbler lock, but with a second independent locking mechanism.

- Manipulation is possible but extremely difficult. Some people can pick these in under a minute. Most people cannot.
- We will focus on **key duplication** and the implications thereof.

1. Reverse-engineering the Primus
2. 3D modeling Primus keys
3. Fabricating Primus keys
4. What it all means

Security through patents

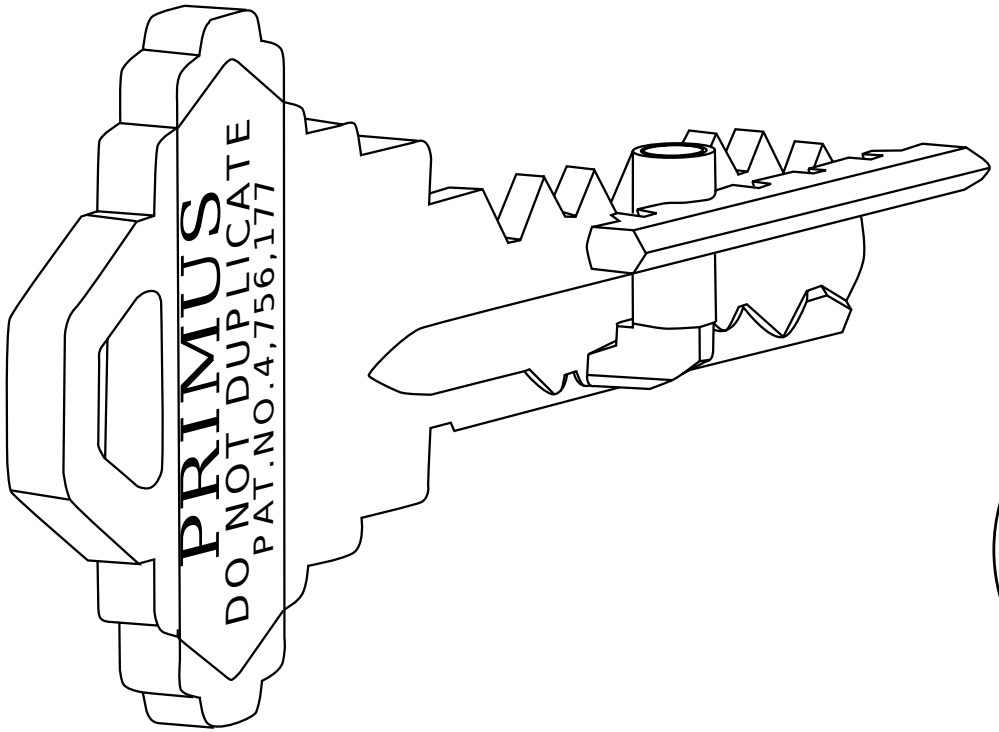
Look up the patent. . .

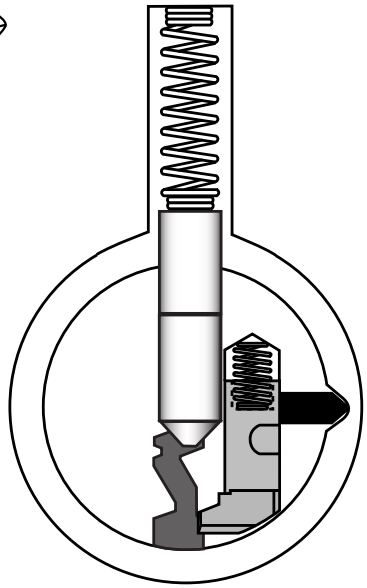


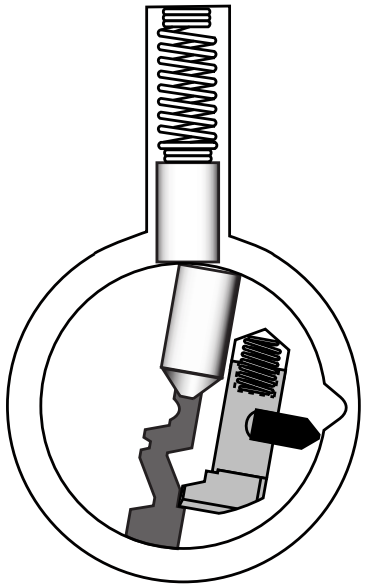
Primus service manual

w3.securitytechnologies.com/IRSTDocs/Manual/108482.pdf
(and many other online sources)

Sidebar operation







- Finger pins must be lifted to the correct height.
- Finger pins must be rotated to the correct angle.

Disassembly

Fill in any missing details by obtaining a lock and taking it apart.

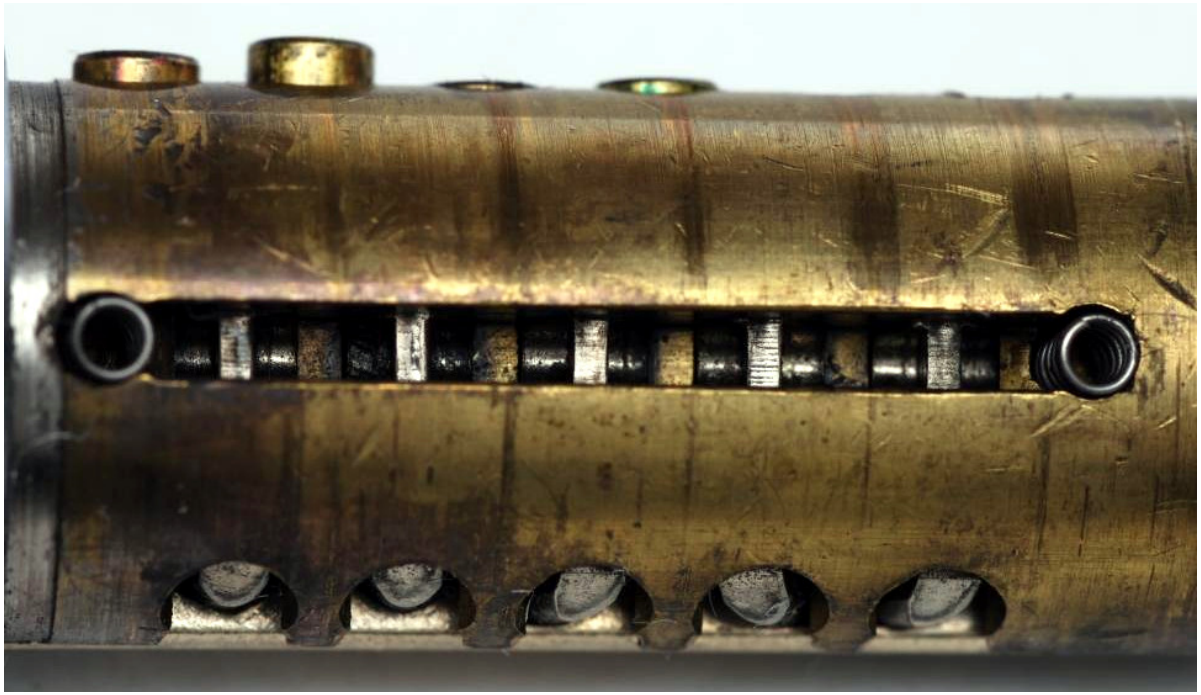
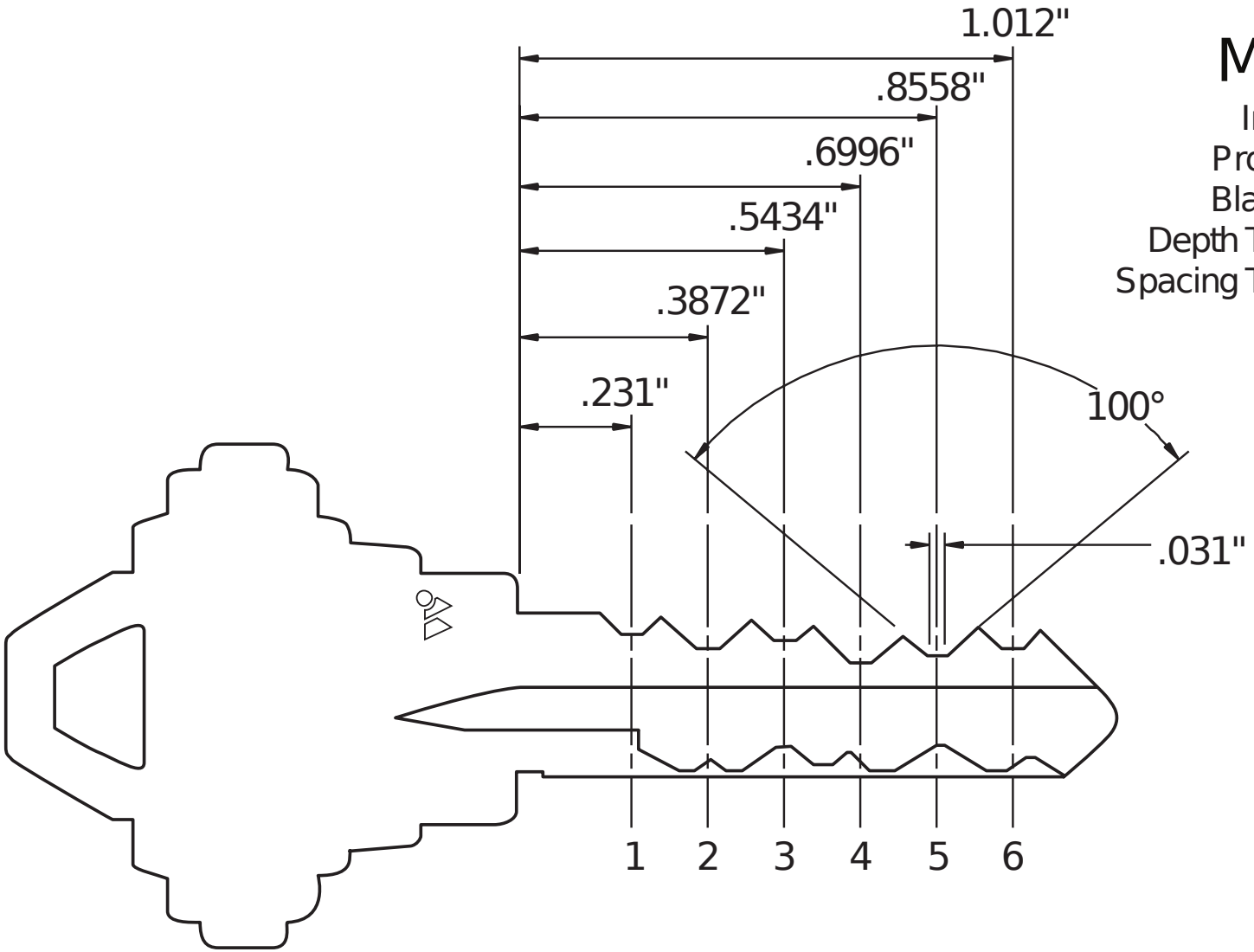


Photo credit: user datagram on `lockwiki.com`. Licensed under CC-BY-3.0.

Top bitting specifications



MACS = 7

Increment:	.015”
Progression:	Two Step
Blade Width:	.343”
Depth Tolerance:	+.002”-0”
Spacing Tolerance:	±001”

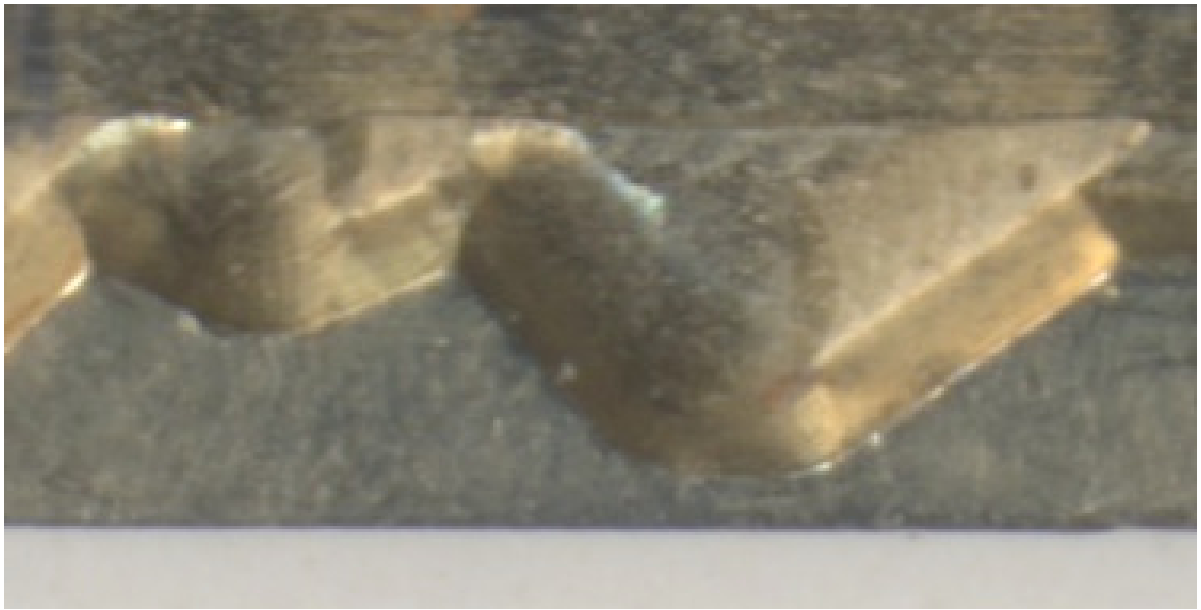
0	.335”
1	.320”
2	.305”
3	.290”
4	.275”
5	.260”
6	.245”
7	.230”
8	.215”
9	.200”

Side bitting specifications

- Schlage doesn't publish exact dimensions for the side bitting.
- Scan 10 keys on flatbed scanner, 1200 dpi, and extract parameters.

Index	Position	Height from bottom	Horizontal offset
1	Shallow left	0.048 inches	0.032 inches left
2	Deep left	0.024 inches	0.032 inches left
3	Shallow center	0.060 inches	None
4	Deep center	0.036 inches	None
5	Shallow right	0.048 inches	0.032 inches right
6	Deep right	0.024 inches	0.032 inches right

Modeling the side bitting

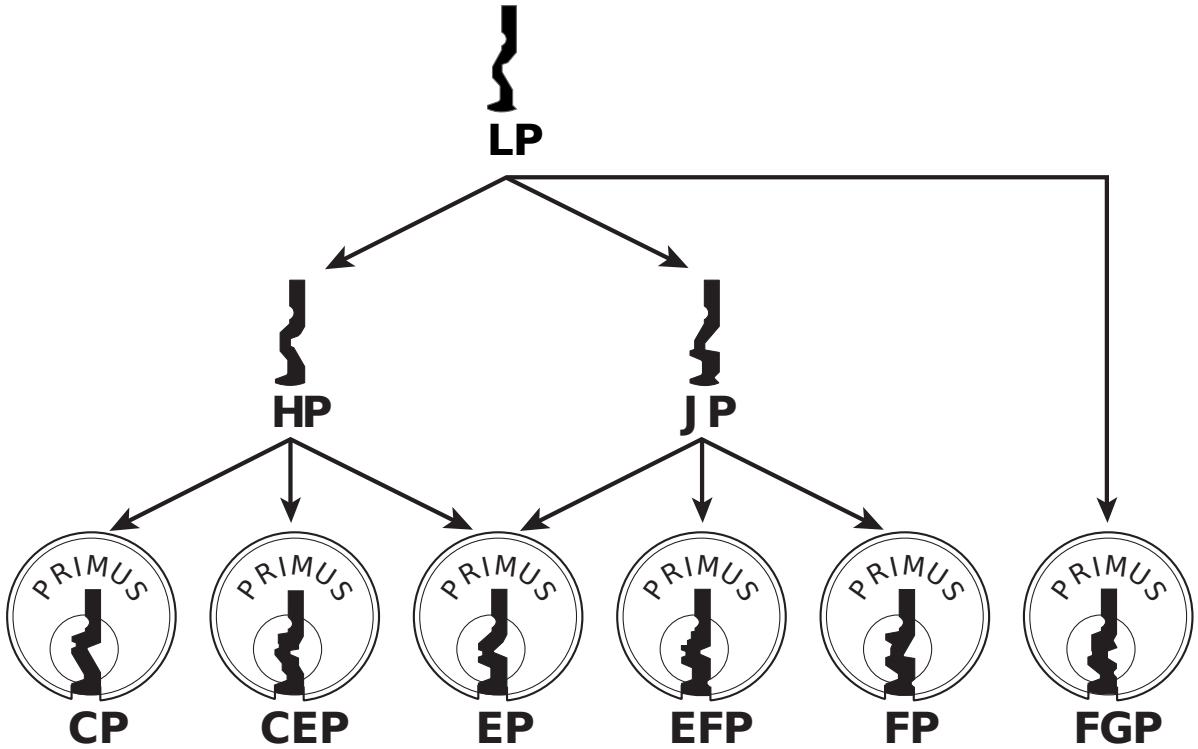


Design requirements

1. Minimum slope: finger pin must settle to the bottom of its valley.
2. Maximum slope: key must go in and out smoothly.
3. Radiused bottom: matches the radius of a finger pin.

Key cross-section

- One shape fits in all Primus locks.
- Dictated by physical constraints: the pins (and therefore the control surfaces) are always in the same place relative to the cylinder housing.



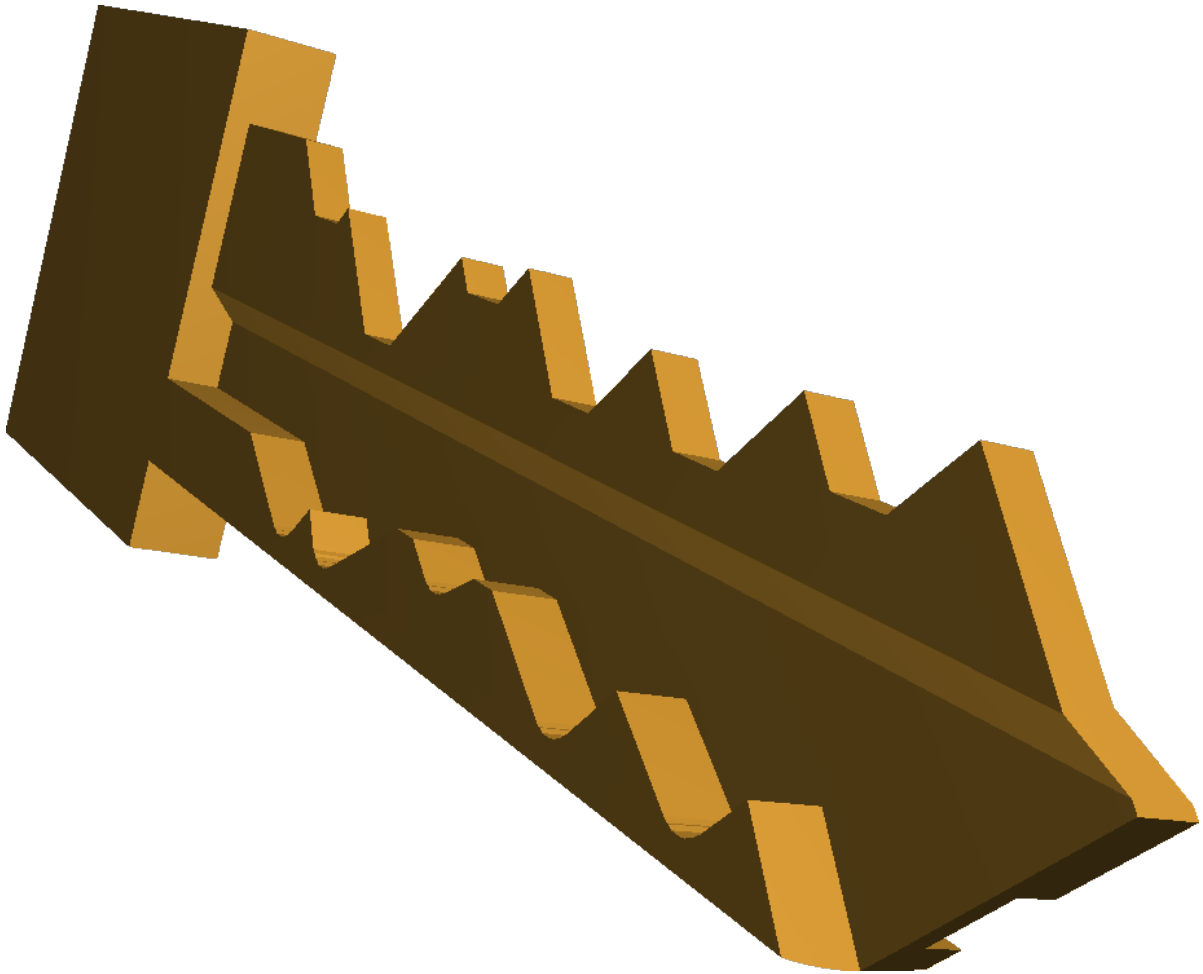
Modeling the key in OpenSCAD

- Programming language that compiles to 3D models.
- First use to model keys was by Nirav Patel in 2011.
- Full implementation of Primus key is a few hundred lines of code.

```
// top_code is a list of 6 integers.
// side_code is a list of 5 integers.
// If control = true, a LFIC removal key will be created.
module key(top_code, side_code, control = false) {
  bow();
  difference() {
    envelope();
    bitting(top_code, control);
    sidebar(side_code);
  }
}
```

The result

```
key([4,9,5,8,8,7], [6,2,3,6,6]);
```



Hand machining

Materials needed:

- Hardware store key blank ($1)
- Dremel-type rotary tool ($80)
- Calipers ($20)

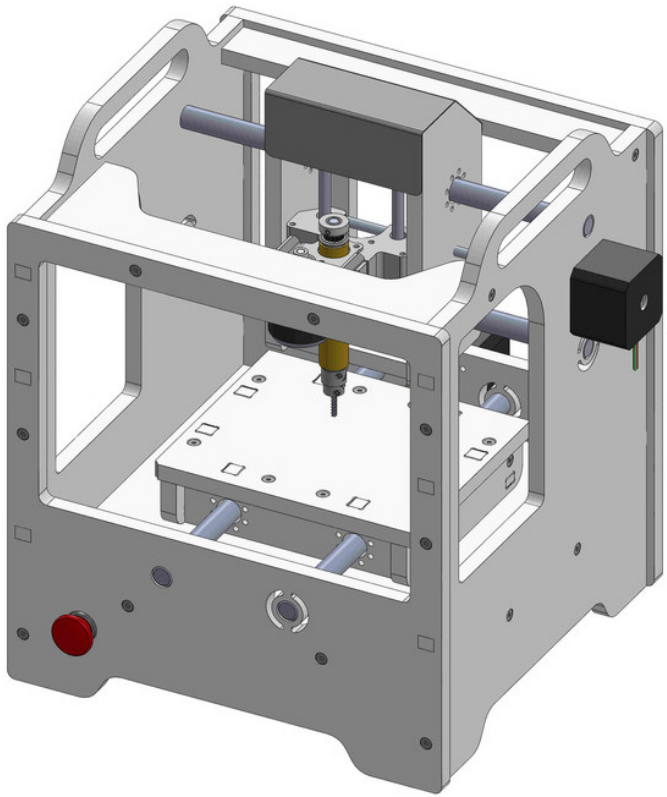
Cut, measure, and repeat ad nauseum.

Rob can crank one out in less than an hour.


20
30
40

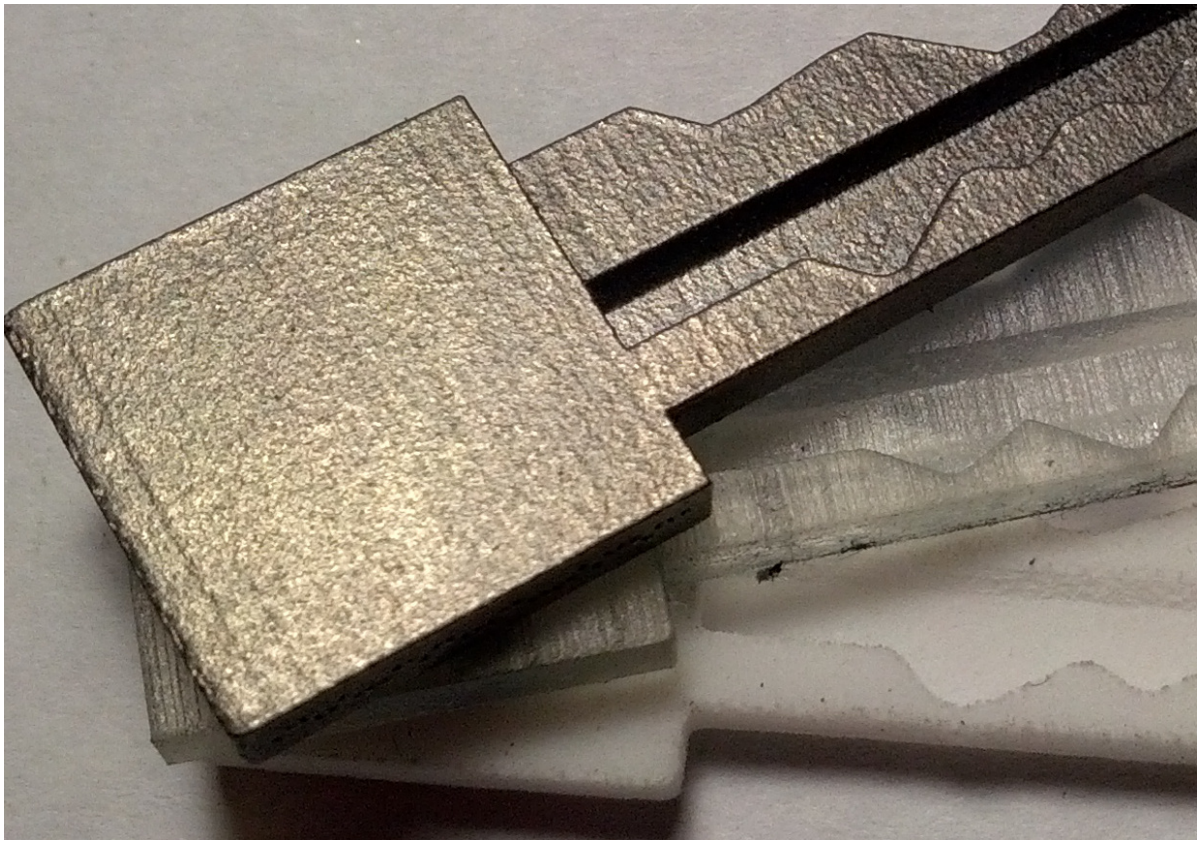
Computer-controlled milling

- This is what the Schlage factory does.
- High setup cost (hundreds of dollars): not practical for outsourced one-off jobs.
- Keep an eye on low-cost precision micromills.



3D printing

This is the game changing technology.



(From bottom to top, picture shows low resolution plastic, high resolution plastic, and titanium.)

3D printing results

- Working keys out of standard plastic (Shapeways "White Strong and Flexible"), high-resolution plastic (Shapeways "Frosted Ultra Detail"), and titanium (from i.materialise) on the first try.
- Plastic keys cost $1 to $5. Some strength issues, but workable.
- Titanium keys cost $100 and outperform genuine Schlage keys.
- Sufficient resolution from all processes.
- Over the next few years, expect to see prices decrease further.

Results

- **Key decoding is easy**: now that we know the dimensions, all you need is a high-resolution photo of a key.
- **Key duplication is easy**: takes $10 and the contents of this talk.
- **Master key extrapolation is easy**: the sidebar is not mastered, so cracking a Primus system is just like cracking a standard pin-tumbler system.
- **Keyless manipulation is still hard**: need to start with at least a photo of a key (or else disassemble a lock).

Our recommendations

- Primus should not be used for high-security applications.
- Existing Primus installations should reevaluate their security needs.

Implications

- The modeling/printing pipeline translates physical security into information security.
- Patent protection defends against physical reproduction, but does nothing about the electronic distribution of 3D models.
- Once a class of keys has been 3D modeled, there is much more power in the hands of unskilled attackers.

Future work

Combine the 3D modeling software with existing image-to-key decoding software and 3D printing services. We envision a one click process: put in a picture that you've snapped of a key and your credit card number, and get the 3D printed key in the mail a week later.

New York City "master keys" debacle: how long until 3D models become available? What will happen then?