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

David Lawrence Eric Van Albert Robert Johnson

locks@mit.edu

DEF CON 21

August 3, 2013

Standard pin-tumbler locks

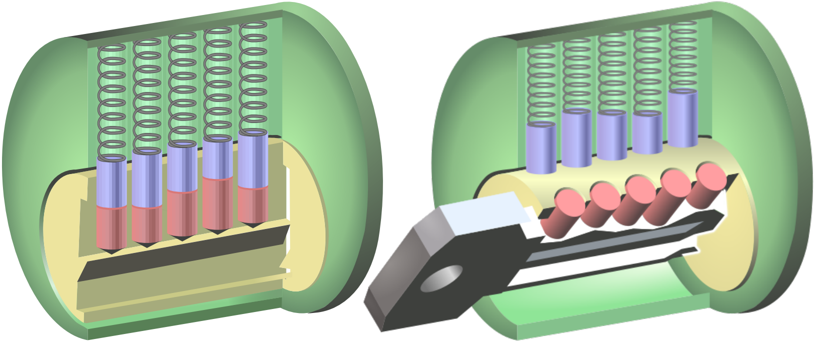


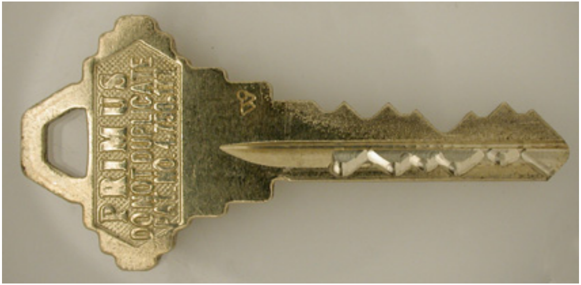
Photo credit: user pbroks13 on Wikimedia Commons. Licensed under GFDL or CC-BY-SA-3.0.

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

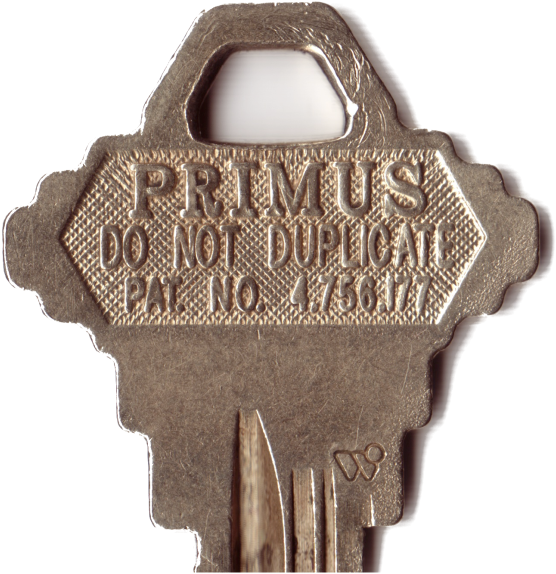
1. Reverse-engineering the Primus

2. 3D modeling Primus keys

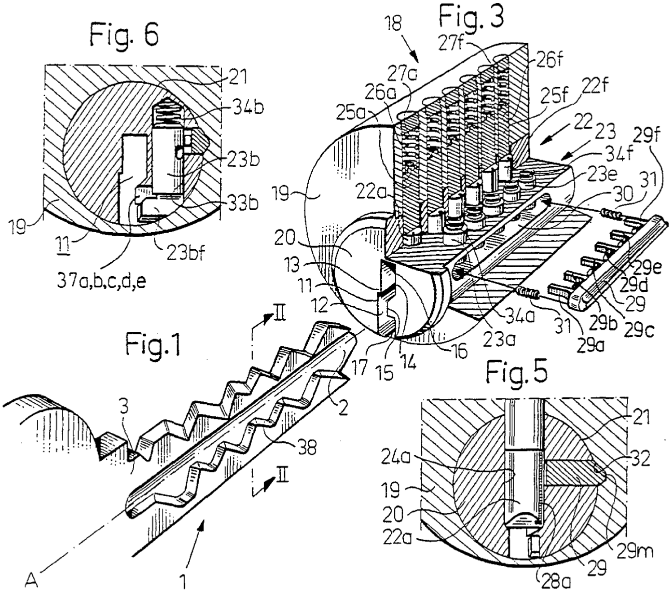
3. Fabricating Primus keys

4. What it all means

Security through patents



Look up the patent. . .



Primus service manual

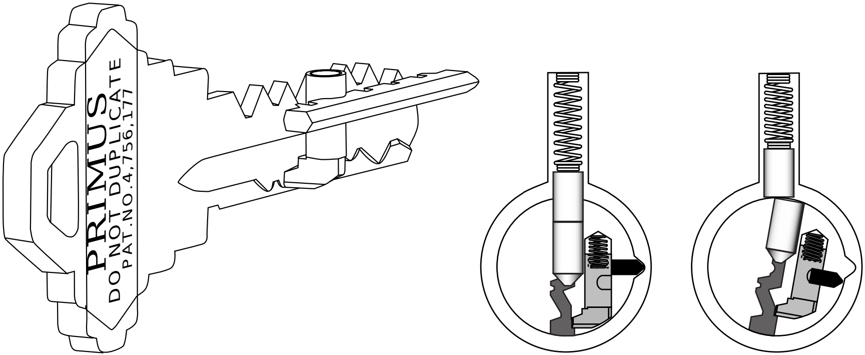
SCHLAGE®

High Security Cylinders & Key Control 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.

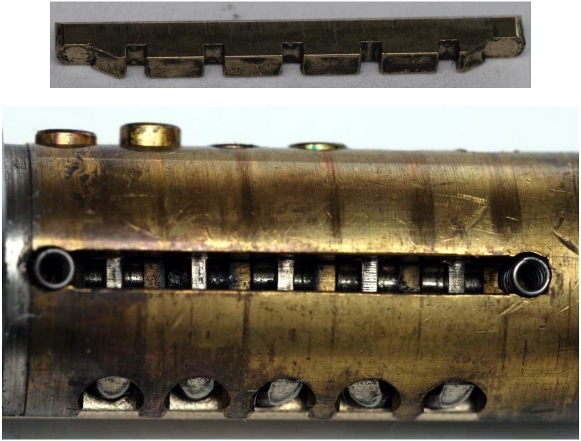


Photo credit: user datagram on `lockwiki.com`. Licensed under CC-BY-3.0.

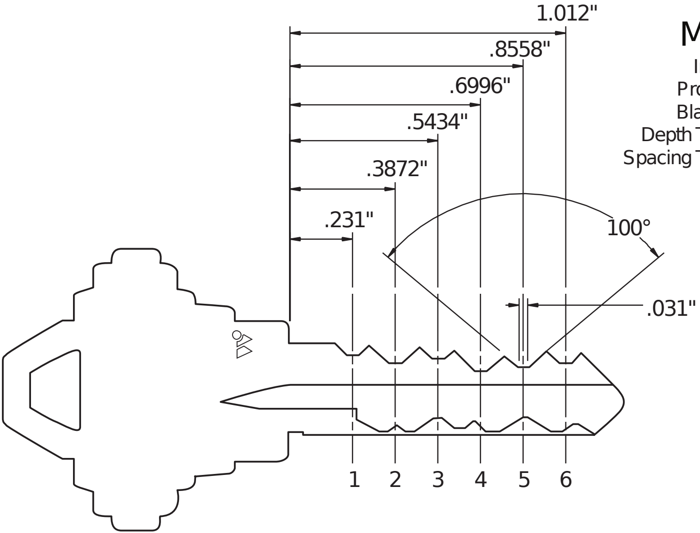
1. Reverse-engineering the Primus

2. 3D modeling Primus keys

3. Fabricating Primus keys

4. What it all means

Top bitting specifications



MACS =7

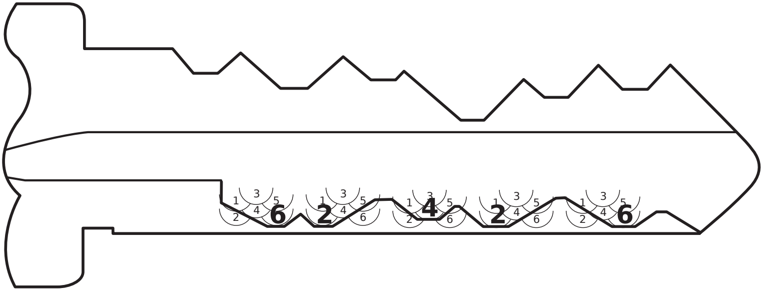
Increment:	.015”
Progression:	Two Step
Blade Width:	.343”
Depth Tolerance:	+.002”-0”
Spacing Tolerance:	±001”

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

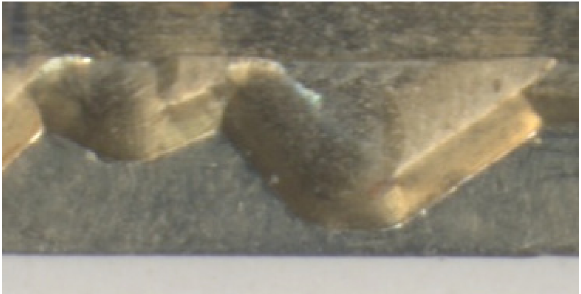
Side bitting specifications

- 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

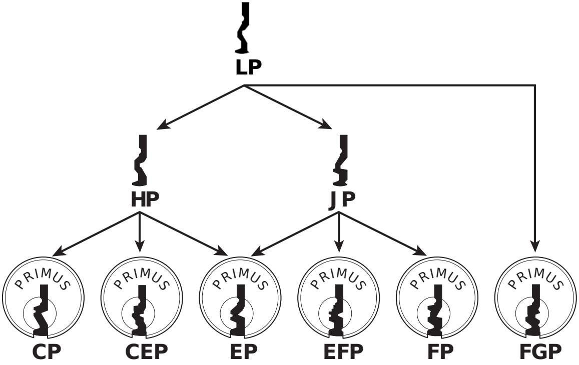


Design requirements

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.



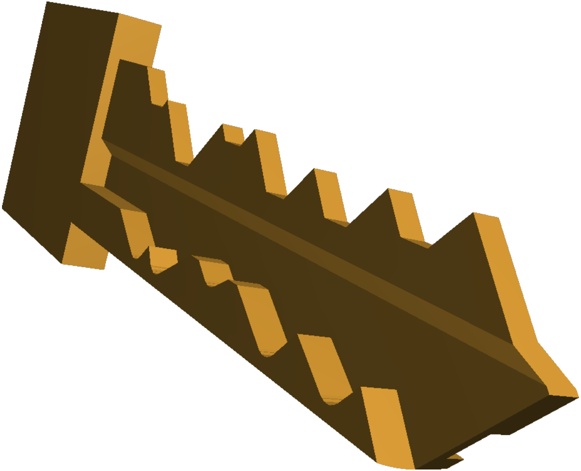
Modeling the key in OpenSCAD

- 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]);
```



1. Reverse-engineering the Primus

2. 3D modeling Primus keys

3. Fabricating Primus keys

4. What it all means

Hand machining

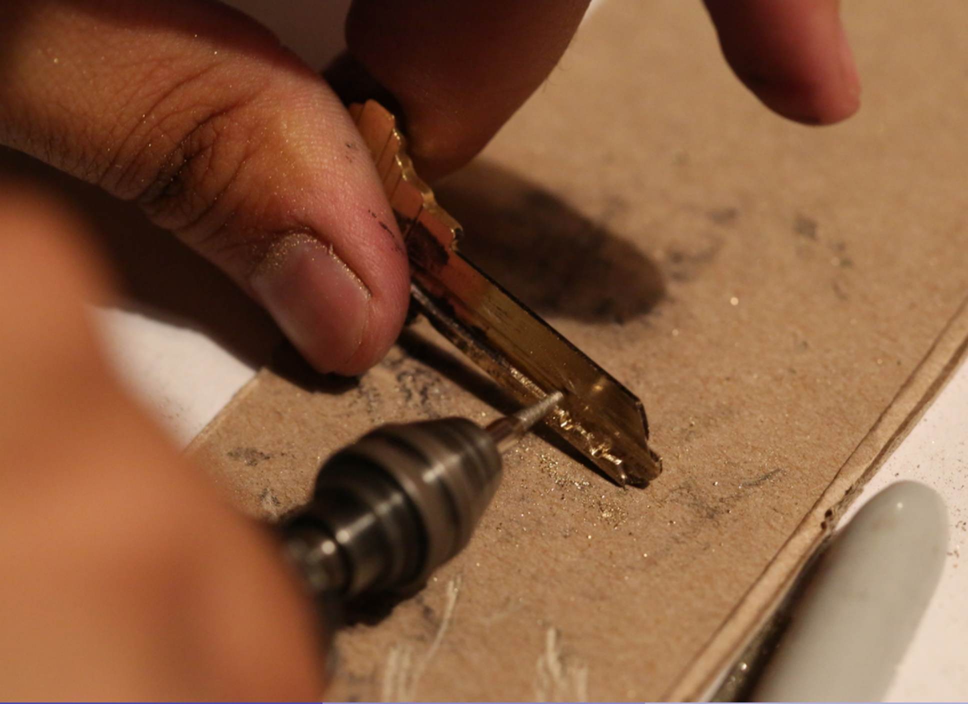
Materials needed:

- 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.

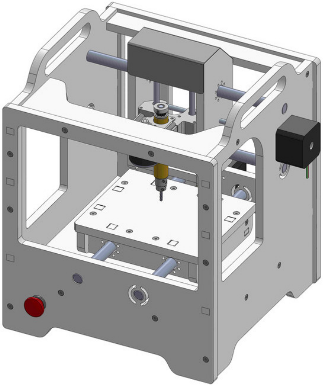
20
30
40



US

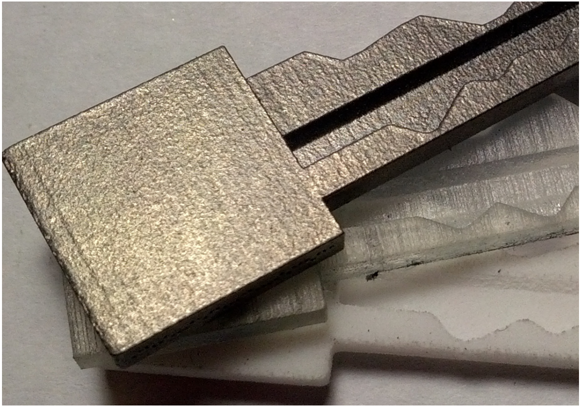
Computer-controlled milling

- 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

1. shapeways.com “frosted ultra detail”
   - $5 setup fee plus $2 per key.
   - Very good precision.
   - Insufficient strength to retract a latch.
2. shapeways.com “white, strong, and flexible”
   - $2 setup fee plus $1 per key.
   - Acceptable precision (operation is less smooth, but it works).
   - Strong enough to operate most locks.
3. i.materialise.com “titanium”
   - $150 per key (ouch!).
   - Very good precision.
   - Very good strength (similar to that of a brass key).

Expect to see prices decrease even more in the near future.

1. Reverse-engineering the Primus

2. 3D modeling Primus keys

3. Fabricating Primus keys

4. What it all means

Primus-specific results

- Key decoding is easy.
- Key duplication is easy.
- Master key extrapolation is easy.
- Keyless manipulation is still hard.

Our recommendations

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

General implications

- This is an industry-wide problem.
- Key duplication will become much more accessible.
- Physical security will depend on information security.
- Patent protection will become less useful.

Figure: A 3D printed car key, by Ryan Weaving,
and a 3D printed disc detainer key, by Nirav Patel.

Audience projects

- Contribute 3D models of other keys. (Medeco, anyone?)
- Integrate 3D models with existing image-to-key decoding software.
- Start a website for the exchange of 3D models of interesting keys.

Tamara Beckwith, NY POST

Figure: New York City "master keys".
What will happen once 3D models of these become available?

Questions?

PRIMUS
POWER
PRIMUS
PRIMUS
POWER GAS
4 Season Mix
2207
PROPANE
ISOBUTANE
BUTANE
Net weight 230 g / 8.1 oz 460 ml
0036