Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding

Benjamin Laxton, Kai Wang and Stefan Savage
Department of Computer Science & Engineering
UCSD

Slides by Alex Nelson

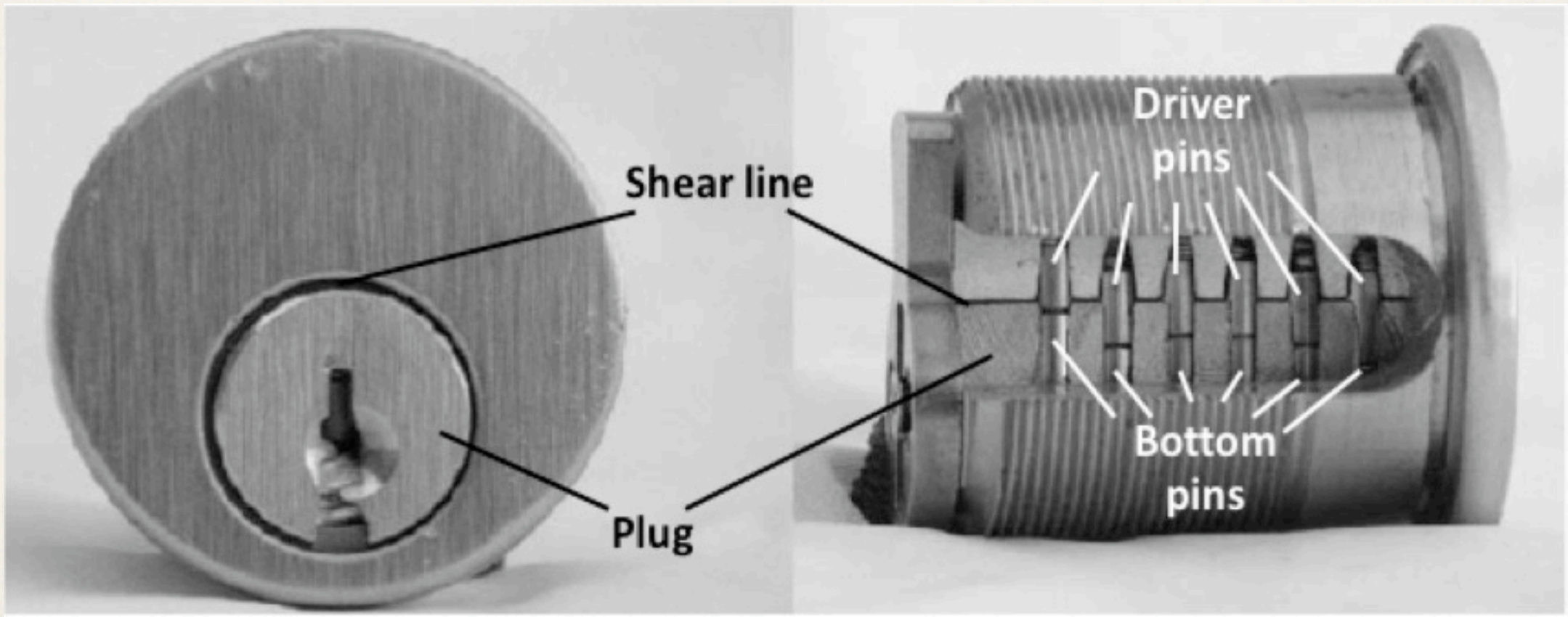
April 28, 2009

Introduction

- Some authentication mechanisms:
  - Something we *are*, *have* or *know*
- Which is a biometric?
  - Schneier: Unique, not secret
    - http://www.schneier.com/blog/archives/2009/01/biometrics.html
- As which “Something” does a key count?

Lock Subversion

- Pin tumbler lock, a design 150 years old;
  - Vulnerable to lockpicking (http://www.liveleak.com/view?i=16e_1240142272)

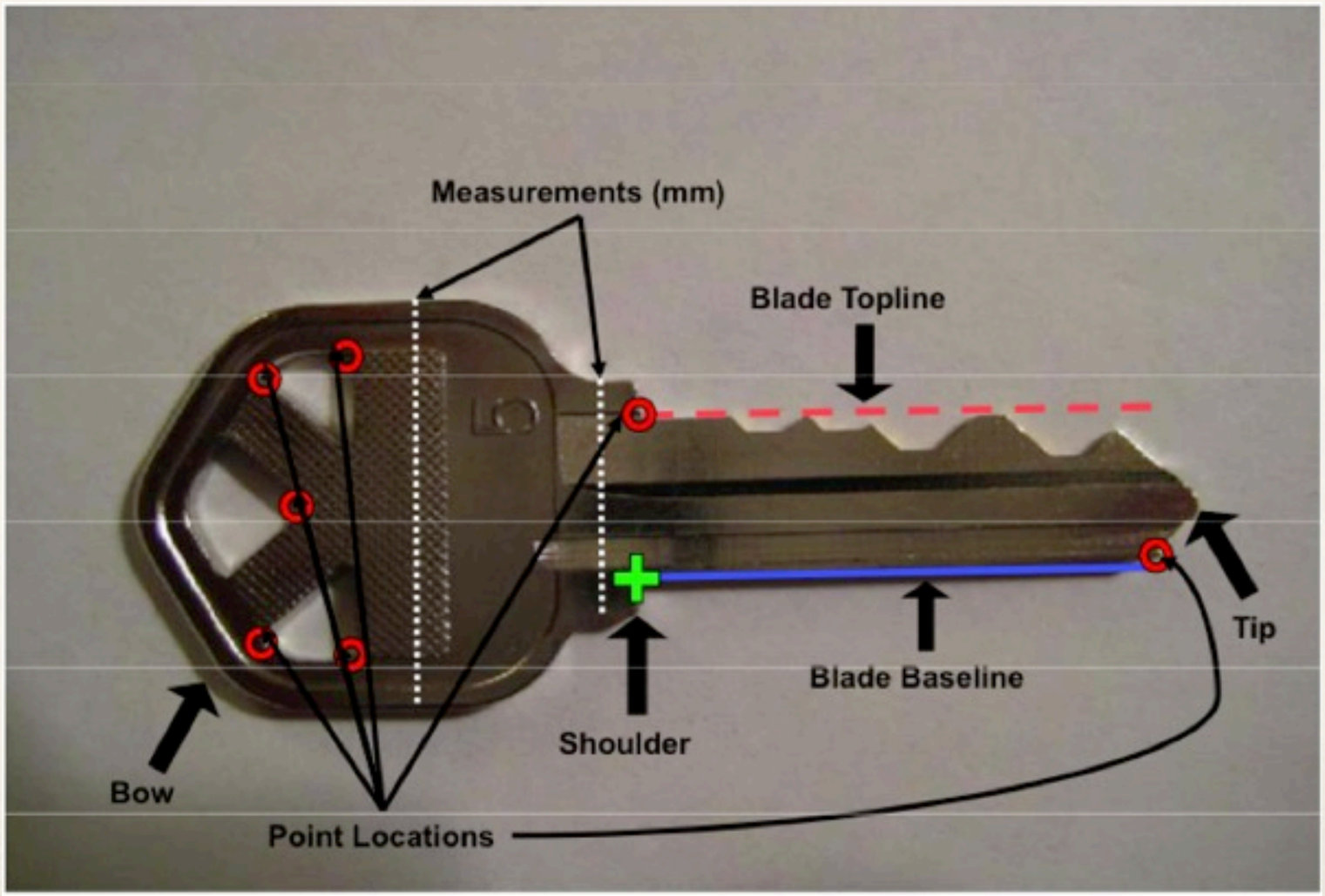


Key Subversion: Hands-On

- Key information: Bitting code
- Acquire, measure, copy

Key Subversion: Hands-Off

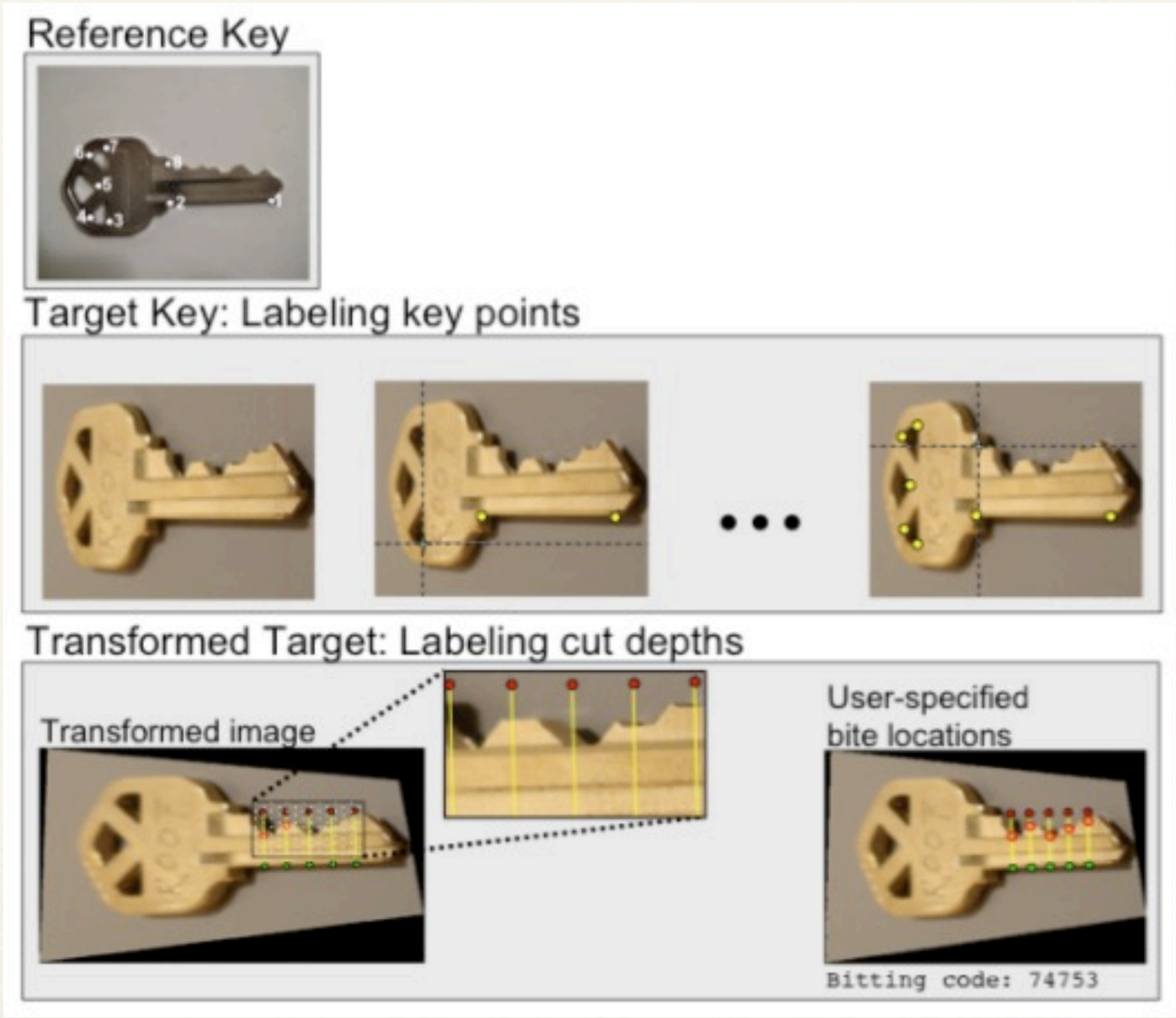
- Teleduplication via optical decoding: Need an image of the target key, a reference key, and a little input



Assumptions for Teleduplication

- 1. The target key "type" is known.
- 2. A key face can be approximated by a 2D plane.
- 3. Absolute metric measurements are known for a reference image of a key.
- 4. A user supplies point correspondences between these reference measurements and their location in the target key.

Sneakey Algorithm: Feature Extraction



Downsides to Sneakey

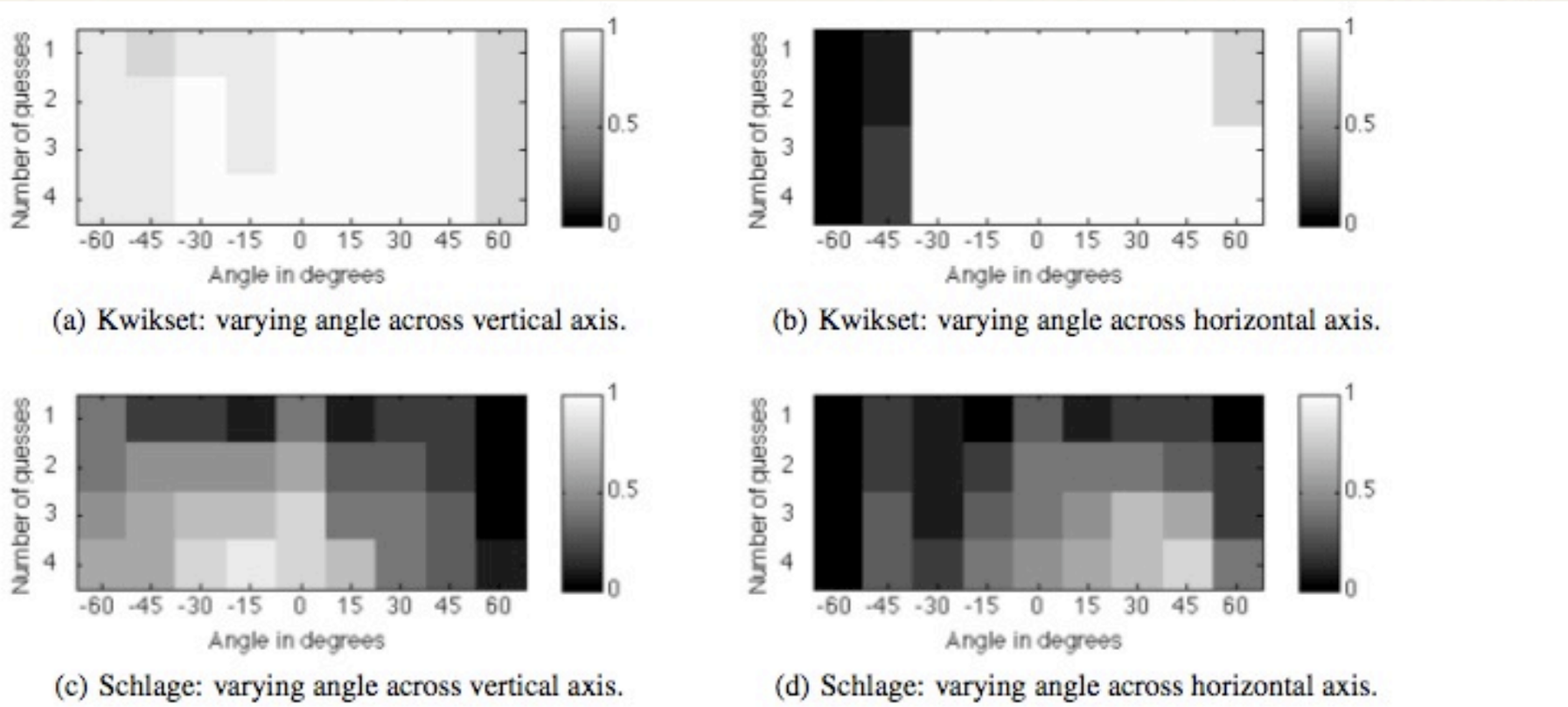
- Not yet fully automated
- Ambiguous depths in photos
  - Guesses necessary

Results: Lab

- Two key types: Kwikset and Schlage
  - Kwikset keys' cut depths further apart
- Point-and-shoot digital camera (circa 2007) at 12 inches from subject, well and consistently lit
- Key images cropped to 1300x850px
- Varying along x and y axes: x left-right in key plane, y up-down

Perspective Impact, x + y Axes

Positive angle definition:
Teeth AWAY from camera on vertical
Teeth TOWARDS camera on horizontal



(a) Kwikset: varying angle across vertical axis.

(b) Kwikset: varying angle across horizontal axis.

(c) Schlage: varying angle across vertical axis.

(d) Schlage: varying angle across horizontal axis.

Figure 6: Impact of perspective on key decoding effectiveness. The shade of each square represents the fraction of key images decoded correctly within the first *n* guesses (indicated on the y-axis) at a particular rotation from a straight-on horizontal viewpoint (indicated on the x-axis).

Surreptitious Cameras: Short-Range

- Cell phone: 2 megapixels
- Tested straight-on, no distortions, 6 inches
- More pixels (1600x1200), but crummier picture (sensor quality)

Manufacturer	1	2	3	4
Kwikset	0.8	1.0	1.0	1.0
Schlage	0.4	0.7	0.8	1.0

Table 1: Fraction of cell-phone captured key images decoded within 1, 2, 3 or 4 guesses for each key type.

Surreptitious Cameras: Long-Range (with Limitations)

- Physical limitations
  - Diffraction: Limits resolution of pairs of lines per millimeter
  - Sensor: Limits arcsecond resolution per pixel
    - (1 arcsecond: resolution of 1mm at 676 feet)
- Pragmatic limitations
  - Good, long glass is big. (How big? ...)

Surreptitious Cameras: Long-Range

Figure 7: Telephoto setup consisting of C5 spotting scope, Tele-vue PowerMate 4X Tele-extender, and Cannon 40D Digital SLR. Entire system folds up into two small cases and weighs 16 pounds.

Surreptitious Cameras: Long-Range, with Style

- http://www.boingboing.net/2006/12/07/leica-rifle-camera.html

Resolution Reminder

Figure 9: Our proof-of-concept telephoto experiment. The key image, captured at a distance of 195 feet, was correctly decoded as 74753.

- Textbook: Marc Weber Tobias. Locks, Safes and Security: An International Police Reference.

Results: Long-Range

Figure 8: Sample key in telephoto experiment, captured at a distance of 35, 65 and 100 feet. The bitting code is 63134.

Viewing Distance	1	2	3	4
35ft	1.0	1.0	1.0	1.0
65ft	0.8	1.0	1.0	1.0
100ft	0.7	0.9	1.0	1.0

Table 2: Fraction of captured key images decoded within 1, 2, 3 or 4 guesses at each distance.

- Long-range photos of ten keys, on a ring, on a café table.
- Time for a key wallet?

Conclusion

- Keys are a secret, waved about in public, at authentication points
- Harvesting these secrets now demonstrated possible
  - Recall also video surveillance, X-Ray machines
- Time for more information in the key
  - RFID in keys for cars
  - RFID in keys for door locks (Medeco's E-cylinder)
  - When is a key not merely "Something we know"?