



# COMPROMISE OF CONVENTIONAL MASTER KEY SYSTEMS

- ◆ Extrapolation of the TMK
- ◆ Other techniques
  - Shimming
  - Decoding



# TOPICS AND OUTLINE

- ◆ Why important;
- ◆ What is a MK system;
- ◆ How locks are Master Keyed;
- ◆ Inherent security of cylinders: general and specific issues (pin tumbler mainly);
- ◆ Overview of compromise of locks and systems;



# TOPICS AND OUTLINE

## ◆ Theory

- How accomplished
- Differs
- Levels of keying
- Incidental master keys
- Cylinders: double pinning
- Standard techniques to MK
- High security locks



# TOPICS AND OUTLINE

- ◆ Extrapolation
- ◆ Special tools and techniques
- ◆ Easy entrie profile milling machine



# MASTER KEYING: WHY IMPORTANT

- ◆ Every large facility is master keyed
- ◆ Compromise of TMK
  - No risk
  - All locks
  - Absolute access
  - Not high tech
  - No forensic trace
  - No time limit to obtain




# What is Master Keying

- ◆ Change keys
- ◆ Incidental master keys
- ◆ Top Level Master Keys
- ◆ Levels of master keying
- ◆ Security v. convenience
- ◆ Security rules against master keying



# HOW ARE LOCKS MASTER KEYED: General Information

- ◆ Locks that can be master keyed
  - Lever
  - Wafer
  - Pin tumbler
  - Hybrid
- ◆ Types of master key systems
- ◆ Why are locks master keyed
- ◆ Other forms of keying



# Access Restrictions and Inherent Security for Cylinders

- ◆ Levels of keying
- ◆ Keyways:
  - Restricted or unique (Everest, 3M)
  - Paracentric
  - Sectional
  - Number of combinations (differs) available
  - Design of blanks, difficulty in replicating
  - Different sidebar codes and blocking





# Master keying: General Security Issues

- ◆ Exposure to lost master keys
- ◆ Reduced pick resistance
  - Double pinning means more chances to pick
- ◆ Unwanted cross keying, key interchange, or incidental master keys
  - keys from the same or other systems may open more locks than intended
- ◆ Unauthorized rights amplification
  - turn a change key into a master key



# Master keying: General Security Issues

- ◆ The security of keys, locks, and code data;
- ◆ Inability to gain access to a cylinder to disassemble it;
- ◆ Ease in decoding a disassembled cylinder. Corbin master ring is good example;
- ◆ How long ago was the system implemented. The average life of a master key system is fifteen years, although many have been in use for a much longer period;



# MK Security Design

- ◆ Secondary locking system and security enhancements;
- ◆ Ability to alter sidebar codes within one master key system;
- ◆ Access control systems that are operated in parallel with mechanical locks;
- ◆ Proprietary keyways that are protected by patent and copyright;



# MK Security Design

- ◆ Difficulty in replicating blanks;
- ◆ Side millings;
- ◆ Undercuts (Schlage Everest);
- ◆ Specially designed ward patterns and activation of sliders (Medeco M3) or mechanically linked sidebars have been implemented;
- ◆ Secondary locking mechanisms and the apparent difficulty in replicating restricted blanks may not actually provide the expected level of security;



# MK Security Design

- ◆ System monitoring and access restrictions;
- ◆ Common areas that are accessible to the public are on the TMK;
- ◆ Ability for change keys to be modified to become a master key or TMK;
- ◆ Unauthorized access to code data for the system;
- ◆ Security of cylinders, physical access;
- ◆ Implementation of two or more systems of physical security within the lock that operate independently and in parallel with each other;



# Security of the Specific MK System

- ◆ Master key and change key design
- ◆ Design of the top level master key;
- ◆ Total number of useable combinations within the system;
  - type of progression
  - minimum depth increment (one or two-step),
  - number of available chambers
  - MACS rules;
- ◆ Type of master key system (total position progression, rotating constant);
- ◆ The number of individuals that have access to master keys and top level master keys;





# Compromise of MK Systems

- ◆ Access to the master key to copy, photograph, or physically decode;
- ◆ Access to one or more cylinders (with or without a change key) for the purpose of decoding the pin segments;
- ◆ False pin-lock decoder to measure pin segments through the use of shim wires;
- ◆ False pin-and-cam pin-lock decoder. This tool allows the probing of each tumbler for its position at shear line. It will also allow the operative to quickly decode a master keyed cylinder to extrapolate the TMK and to generate a key;

# Additional methods to Obtain the TMK

- ◆ Shim the cylinder with depth keys to determine the code for each pin segment. This method requires access to the cylinder shear line for the insertion of a shim wire;
- ◆ Visual inspection of the pin tumblers;
- ◆ Optical devices to view the tumblers;
- ◆ Radiographic techniques;
- ◆ Analysis of one or more change keys to reverse engineer the system;
- ◆ Extrapolation and decoding through the use of a change key;







# MASTER KEYING THEORY

# MASTER KEYING



Sometimes more than one key can operate a lock  
Institutions like to have *master keys* that open entire groups of locks.

*Change Keys* operate just one lock

The *Top Master Key (TMK)* operates all locks

There may be more than one level of mastering  
sub-master, grand-master, great-grand-master, etc.  
may overlap (3<sup>rd</sup> floor master, electrical closet master)





# Master Keying Methods

- ◆ Some ways to master key locks
- ◆ Install 2 or more cylinders, linked together
  - one keyed to change key, others to master(s)
- ◆ Special lock design – “master rings”
  - requires special lock (expensive)
- ◆ Use only a subset of pins for change keys
  - grossly reduces security
- ◆ Add extra “master” cuts to pin stacks
  - most common technique, subject of this talk

# DIFFERS

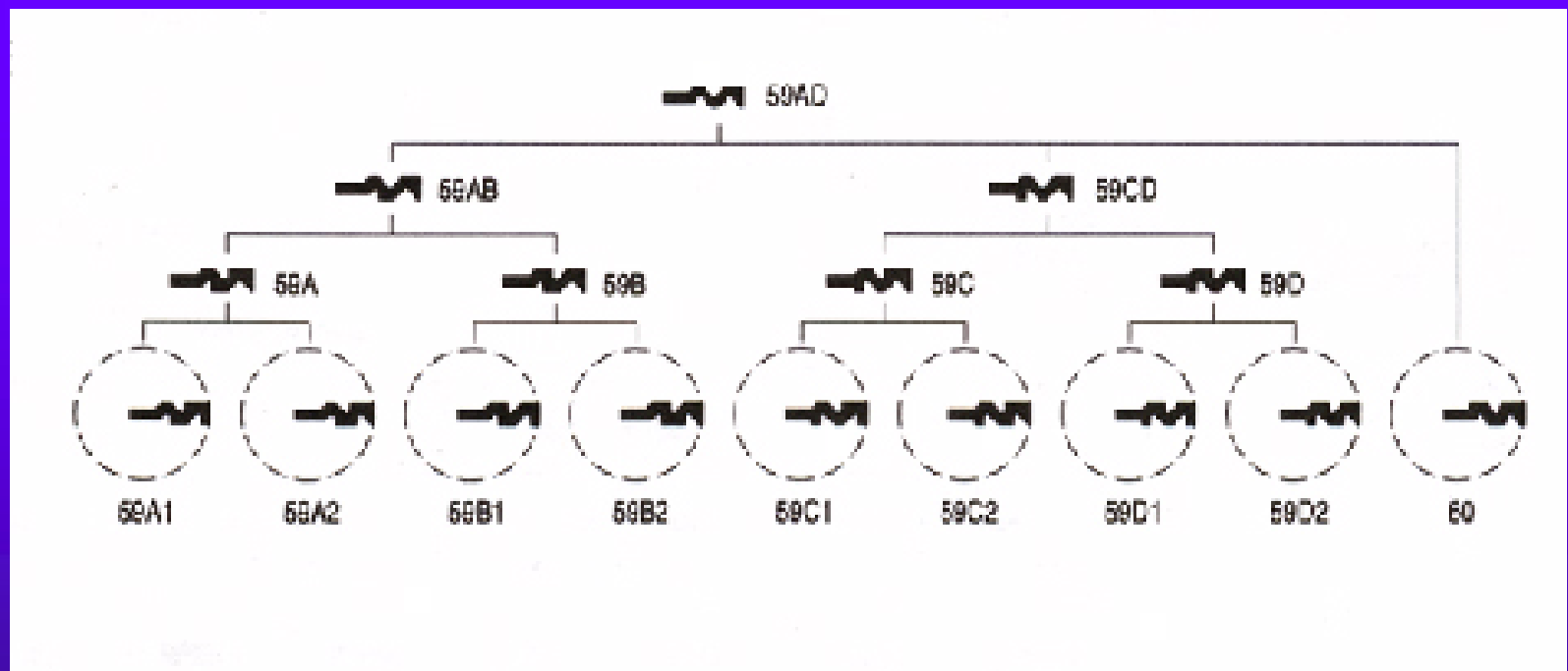


A  = m 10

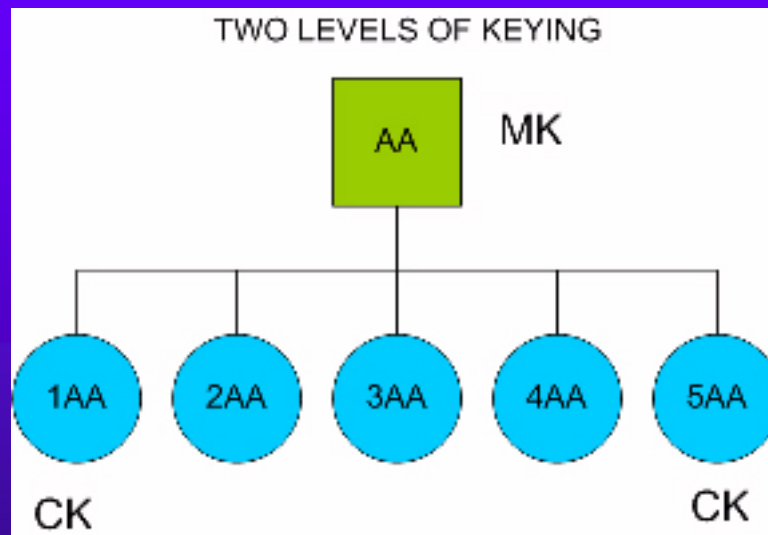
B  = n 5

$V = m^n$   $10^5 = 100.000$

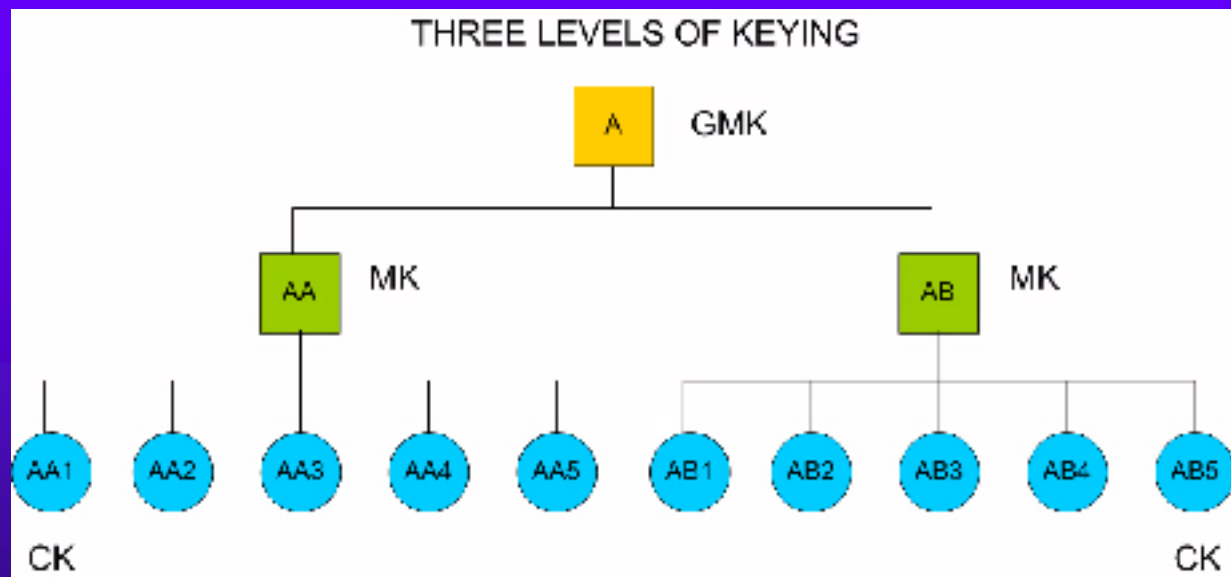
# SECTIONAL KEYWAYS



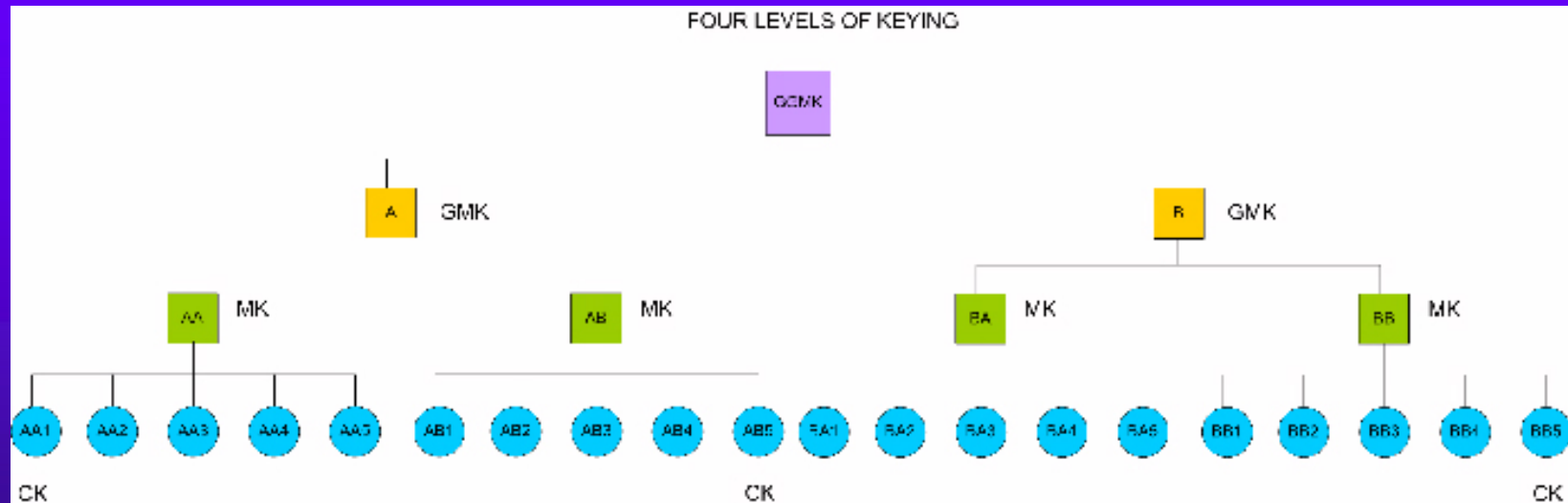
# TWO MK LEVELS



# THREE MK LEVELS



# FOUR MK LEVELS



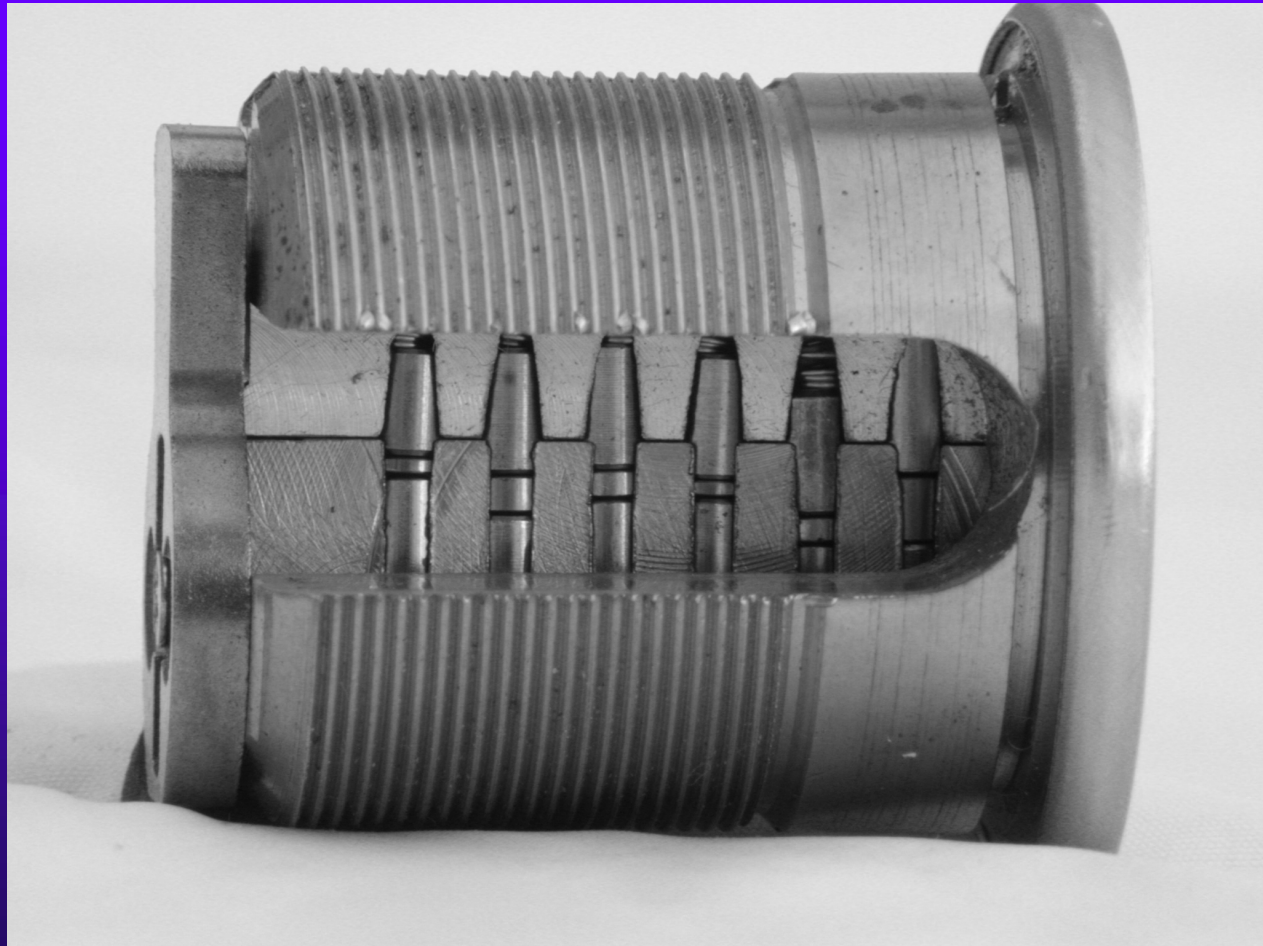




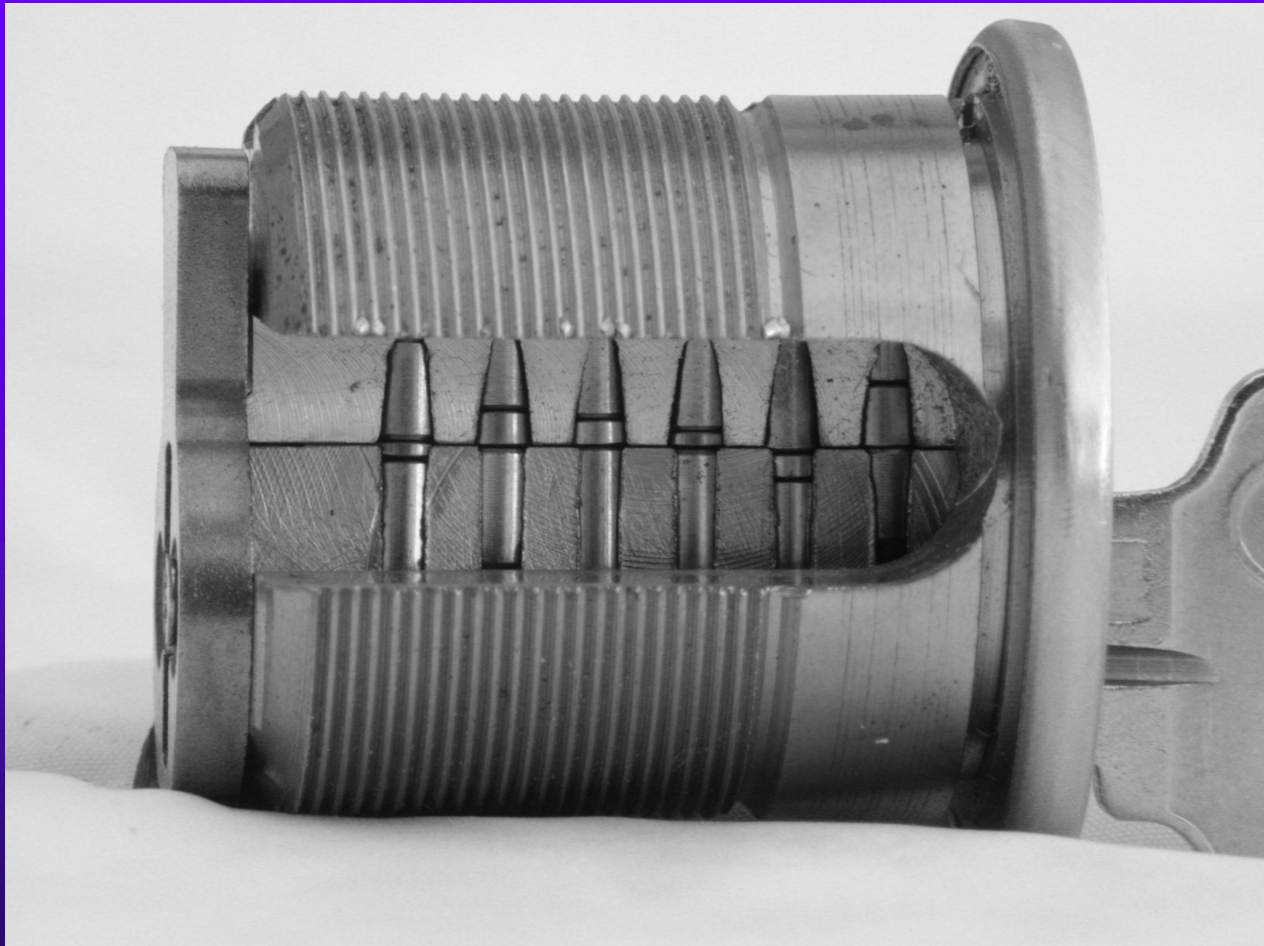
# Problems Encountered

- ◆ TPP, RC, or PPP not utilized
- ◆ More than two lower pins
- ◆ Change key is really a master key
- ◆ Sampled lock not related to target lock
- ◆ Target is not on MK system
- ◆ Target is not on TMK
- ◆ Multiple sidebar codes

# Two Lower Pins



Set of pins raised to shear line





# Example: pin combinations

- ◆ Lock *A* has pins 1-5 cut at heights 1 and 2
- ◆ Lock *B* has pins 1-5 cut at heights 2 and 4
- ◆ Key 11111 is a change key for *A*
- ◆ Key 44444 is a change key for *B*
- ◆ Key 22222 is a master key for both
- ◆ Actually,  $2^5$  keys operate each lock
  - 12121 opens lock *A* (but not lock *B*)



# Standard Techniques

- ◆ Total Position Progression (TPP)
  - every pin stack has two cuts
  - no change key uses a master cut in any position
- ◆ Rotating Constant (RC)
  - every change key uses the master cuts in the same number of positions (C)
  - C pin stacks in each lock have only the master cut; the rest have two cuts
  - the particular positions vary (“rotate”) from lock to lock
- ◆ Partial Position Progression (PPP)  
Hybrid of TPP and RC





# Incidental Master Keys

- ◆ Composite of break points of CK and MK
- ◆ TPP, RC, PPP Systems
- ◆ TPP: Never share values of the TMK



# Two Lower Pins in each Chamber

- ◆ TPP guaranteed results
- ◆ If not change key, then TMK
- ◆ RC somewhat more complicated
- ◆ 5 keys or less to compromise system
- ◆ Use change key as a constant



# High Security Locks and Master Key Systems

- ◆ Why are they rated
- ◆ Forced entry
- ◆ High security and MK systems
- ◆ Surreptitious Entry
  - Picking
  - Decoding
  - Impressioning
  - Extrapolation





# EXTRAPOLATION: THREAT TO SECURITY



# EXTRAPOLATION DEFINED

- ◆ Use of any change key as a constant to probe sampled and target cylinders
- ◆ What is a change key
- ◆ What is a TMK
- ◆ What is an incidental master key



# Some Practical Considerations

- ◆ Total cost of attack: \$2.00 or less
- ◆ Blanks can be cut with a file or a machine
- ◆ Blanks are readily available for most locks
- ◆ Some systems don't follow standard mastering practices (TPP, RC)
  - usually this makes the attack even easier
- ◆ Yes, it really works



# Extrapolation: Read the Lock

- ◆ Requires access to a single lock and its key
  - plus a few blank keys
- ◆ No disassembly or skill required
- ◆ Simple idea
  - a lock is an oracle that accepts or rejects keys
  - lock behaves the same way whether pins are at master or change height
  - learn the master height one pin at a time



# EXTRAPOLATION

- ◆ Derive the code of the Top Level Master Key (TMK)
- ◆ What is a master key system
- ◆ What is the difference between conventional and positional master key systems
- ◆ Why is this so critical



# EXTRAPOLATION OVERVIEW

- ◆ Simple premise
- ◆ Easy to accomplish
- ◆ Much publicity
- ◆ NY TIMES, January 2003
- ◆ Serious threat to security
- ◆ Most buildings use conventional master keying



# EXTRAPOLATION OVERVIEW

- ◆ No special tools
- ◆ No special expertise
- ◆ Common implements
- ◆ Totally covert
- ◆ No forensic traces
- ◆ Can be accomplished over time
- ◆ Access to one change key





# Extrapolation Theory: Overview

- ◆ Conventional systems: split pin master keying
- ◆ Virtual shear lines created by each pin segment within each pin stack
- ◆ Different combinations: incidental master keys
- ◆ No more than two lower pins



# Rights Amplification Concept

- ◆ Computer concept;
- ◆ If you can turn a change key into a master, there's little point in having change keys;
  - might as well have all locks keyed alike
- ◆ A primary security objective of locks is to control insider access;
  - give access to some places but not others



# Modes of Attack: Rights Amplification

- ◆ Take a lock apart and measure cut heights
  - the cut that doesn't correspond to change cut at each position is the master
  - conspicuous, risk of improper reassembly
- ◆ TPP systems: conspire with friends
  - get a bunch of change keys and measure them
  - the “unused” height at each position is the master
  - works only against TPP systems and also requires that attacker have friends



# The Attack

- ◆  $P$  is number of pins,  $H$  is number of heights
- ◆ For each pin  $p$  from 1 to  $P$ 
  - for each height  $h$  from 1 to  $H$ 
    - prepare a test key cut as the change key at every position except  $p$
    - at position  $p$ , cut height  $h$
    - try the key (ask the oracle)
- ◆ Each working test key corresponds to master key height at the position under test



# A Simple Optimization

- ◆ Consumes  $P(H-1)$  blank keys
- ◆ Only need  $P$  blanks
  - re-use blanks at each position
  - start by cutting position  $p$  to tallest height
  - cut it down by one height after testing
- ◆ Still requires  $P(H-1)$  probes of lock



# Countermeasures

- ◆ Don't do master keying
- ◆ Sidebars and multiple sidebar codes
- ◆ Use a lock design that resists this attack
  - e.g., master rings (requires special locks)
- ◆ Add “false” cuts to pin stacks
  - increases susceptibility to cross keying
  - but makes it more difficult to learn true TMK



# Protection Against Extrapolation

- ◆ Standard conventional cylinders
- ◆ Positional master keying
- ◆ High security cylinders
  - Sidebars
  - Special blanks
  - Restricted keyways
  - Multiple sidebar codes





# Information Needed

- ◆ Relationship between the target locks to be opened and the lock that is to be tested with the change key biting test keys;
- ◆ Conventional or positional master key system;
- ◆ Multiple sidebar codes (Medeco or Assa)
- ◆ Has a standard method of progression been utilized · Is the target lock on the master key system;
- ◆ Is it certain that a change key is available and that the change key is associated with the target lock;
- ◆ Have standard depths been utilized;



# Information Needed

- ◆ Estimate of the required security of the system;
- ◆ Manufacturer data;
- ◆ Identification of the lock manufacturer;
- ◆ Is a maison-keying system implemented;
- ◆ Local or factory keyed
- ◆ Number of keying levels.
- ◆ Construction keyed cylinders
- ◆ Information from systems that have implemented visual key control



# Information from Change Key

- ◆ Identification of keyway and available blanks;
- ◆ Identification of sectional keyways and all of the potential sub-sections as well as the keyways that control each section and which would be utilized for the TMK;
- ◆ Number of active chambers within each cylinder;
- ◆ Whether a one or two-step progression is utilized;
- ◆ Parity system;
- ◆ Depth and spacing data;
- ◆ Change key code;
- ◆ MACS rules;



# Variables

- ◆ Sectional keyway
- ◆ Selective master keys
- ◆ TPP, RC, PPP
- ◆ Master ring
- ◆ Double pinning
- ◆ No master pins
- ◆ Not master keyed (NMK)



# Variables

- ◆ Violation of minimum depth rules;
- ◆ Single-step progression v. two-step;
- ◆ Different depth increments than expected;
- ◆ Parity rules not followed;
- ◆ Non-standard depth coding;
- ◆ Multiple sidebar codes;
- ◆ KBA error



# Tactical Considerations

- ◆ Extrapolation is the best method · Verification that there is only one master key system;
- ◆ Verification that the change key is to be used for sampling;
- ◆ Verification that the proper blanks have been obtained;
- ◆ Secondary locking mechanism same for target;
- ◆ Within what time frame is the decoded TMK required
- ◆ Verification the number of pins in the sample and target lock are the same;



# Tactical Considerations

- ◆ Only one change key or master key is required. owed and copied or decoded;
- ◆ Access to a cylinder that is associated with the top level master key;
- ◆ If sectional keyways are employed, proper blank is available
- ◆ Ability to reproduce bittings for each sample key.
- ◆ If the Falle pin-lock decoder is being utilized, verification that the proper keyway has been supplied;
- ◆ Determination of the number of samples that can be obtained from the test lock at one time, or over a period of time;
- ◆ Access to more than one cylinder, if required;





# Tactical Considerations

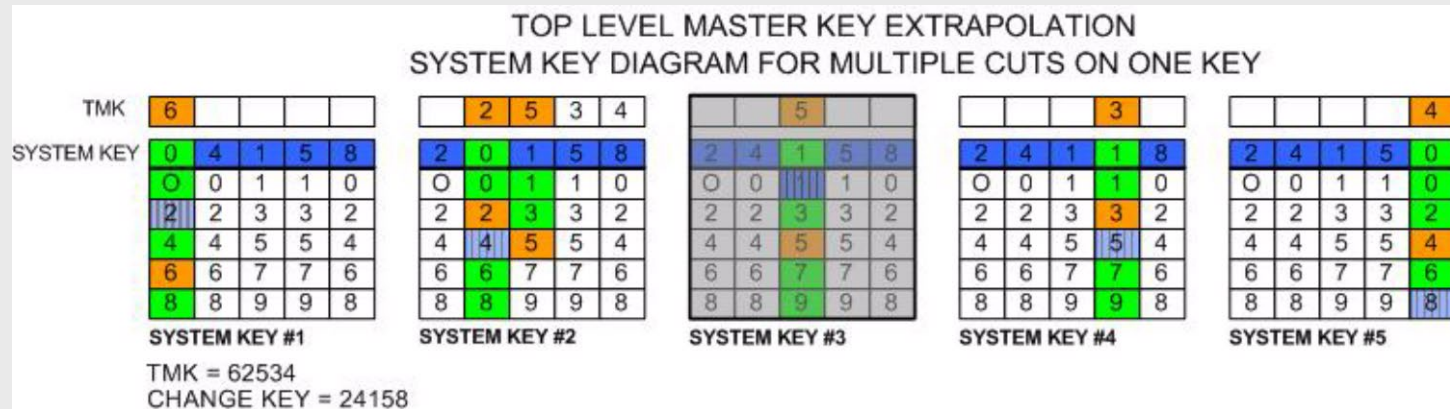
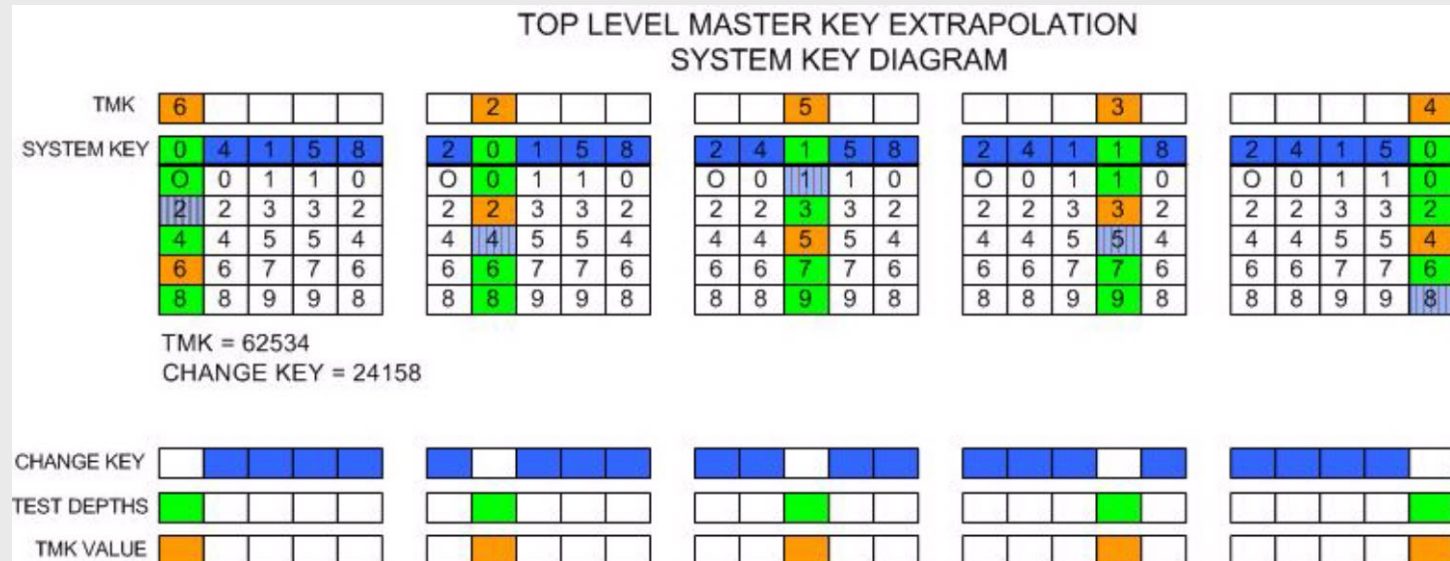
- ◆ Sufficient number of blanks to complete the sample process;
- ◆ The time available for the decoding process
- ◆ The visibility of the sample and target lock;
- ◆ Analysis of the work area
- ◆ The specific location of the target and sample locks;
- ◆ The number of locks to be tested and verified;
- ◆ If reprogrammable locks are installed, such as Instakey, then bottom pins or master pins may be inadvertently removed or parked, thereby changing the combination of the lock and providing a false positive indication of the TMK;



# Decoding Options

- ◆ Decode the TMK with a change key in one session while at the test cylinder;
- ◆ Decode the TMK with a change key in multiple sessions;
- ◆ Decode the TMK with a master key in one session. Up to 32 or 64 keys would be generated in this process, but the actual value of the TMK (which key was the TMK) would not be known;
- ◆ Decode the TMK with a master key in multiple sessions;
- ◆ Shim a cylinder;
- ◆ Utilize the Falle pin-and-cam pin-lock decoder system to decode and possibly generate a working TMK during one session;
- ◆ John Falle Pin lock decoder (original model).

# Decoding in one session





# Pre-cut System Keys for 24158

SYSTEM KEYS FOR CHANGE KEY 24158				
POSITION #1	POSITION # #2	POSITION # #3	POSITION # #4	POSITION # #5
04158	20158	24358	24118	24150
44158	22158	24558	24138	24152
64158	26158	24758	24178	24154
84158	28158	24958	24198	24156

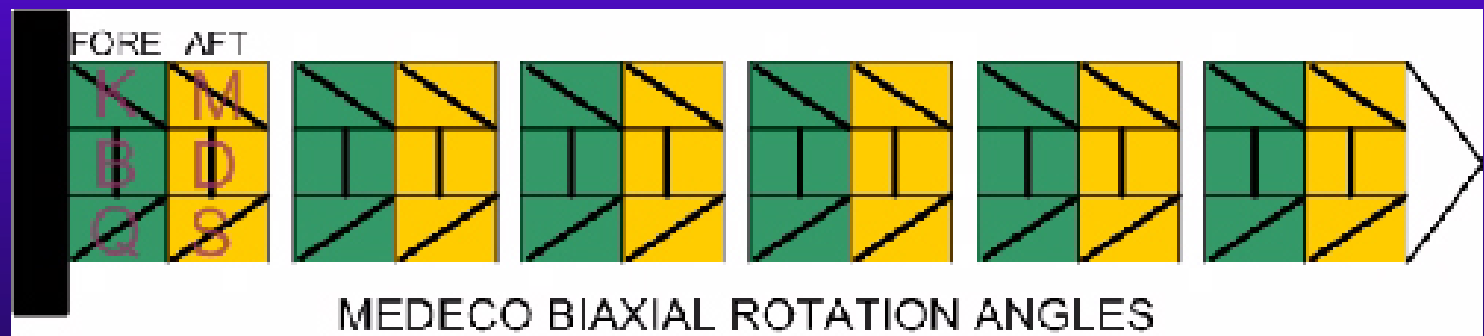


# HIGH SECURITY LOCKS: MEDECO AND ASSA

- ◆ Can add security to a system if implemented properly
- ◆ Can be defeated
- ◆ Why consider these systems
- ◆ Concept of multiple sidebar codes



# Medeco Original and Biaxial



# Medeco Biaxial



MEDECO BIAXIAL MASTER KEY SYSTEM	
MK GROUP	SIDEBAR PATTERN
BASE	K D Q K D Q
GROUP 1	K D Q K D <u>S</u>
GROUP 2	K D Q K <u>B</u> Q
GROUP 3	K D Q <u>M</u> D Q
GROUP 4	K D <u>D</u> K D Q
GROUP 5	K <u>B</u> Q K D Q
TMK	K D Q K D Q - B D M B S



# Medeco Biaxial Double Cut TMK

BIAXIAL MASTER KEY SYSTEM						
TMK	K	B D	Q D	K M	B D	Q S
BASE	K	D	Q	K	D	Q
GROUP 1	K	D	Q	K	D	S
GROUP 2	K	D	Q	K	B	Q
GROUP 3	K	D	Q	M	D	Q
GROUP 4	K	D	D	K	D	Q
GROUP 5	K	B	Q	K	D	Q

# Decoding Biaxial with different sidebar codes: 2+4

IDENTIFICATION OF TWO GROUPS $\times$		
COMPLEMENTARY ANGLES VARIED $\times$	CONSTANT FOR CHANGE KEY $\times$	PERMUTATIONS $\times$
1+2 $\times$	3456 $\times$	45 (3 x 3 x 5) $\times$
1+3 $\times$	2456 $\times$	
1+4 $\times$	2356 $\times$	
1+5 $\times$	2346 $\times$	
1+6 $\times$	2345 $\times$	
2+3 $\times$	1456 $\times$	36 (9 x 4) $\times$
2+4 $\times$	1356 $\times$	
2+5 $\times$	1346 $\times$	
2+6 $\times$	1345 $\times$	
3+4 $\times$	1256 $\times$	27 (9 x 3) $\times$
3+5 $\times$	1246 $\times$	
3+6 $\times$	1245 $\times$	
4+5 $\times$	1236 $\times$	18 (9 x 2) $\times$
4+6 $\times$	1235 $\times$	
5+6 $\times$	1234 $\times$	9 (1 x 9) $\times$

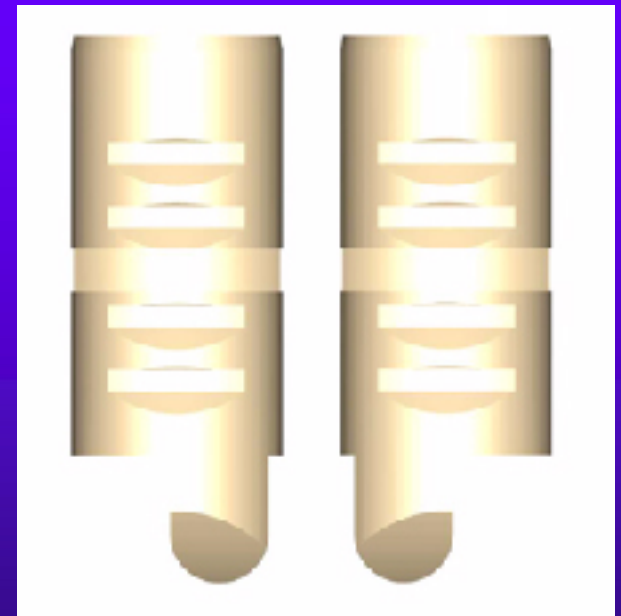




# Decoding Biaxial with Impressioning Information

- ◆ Impression sidebar millings
- ◆ Maximum, 21 keys required
- ◆ Determine differences between sample and target lock
- ◆ Test all samples for differences

# ASSA V10 (7000) SIDEBAR

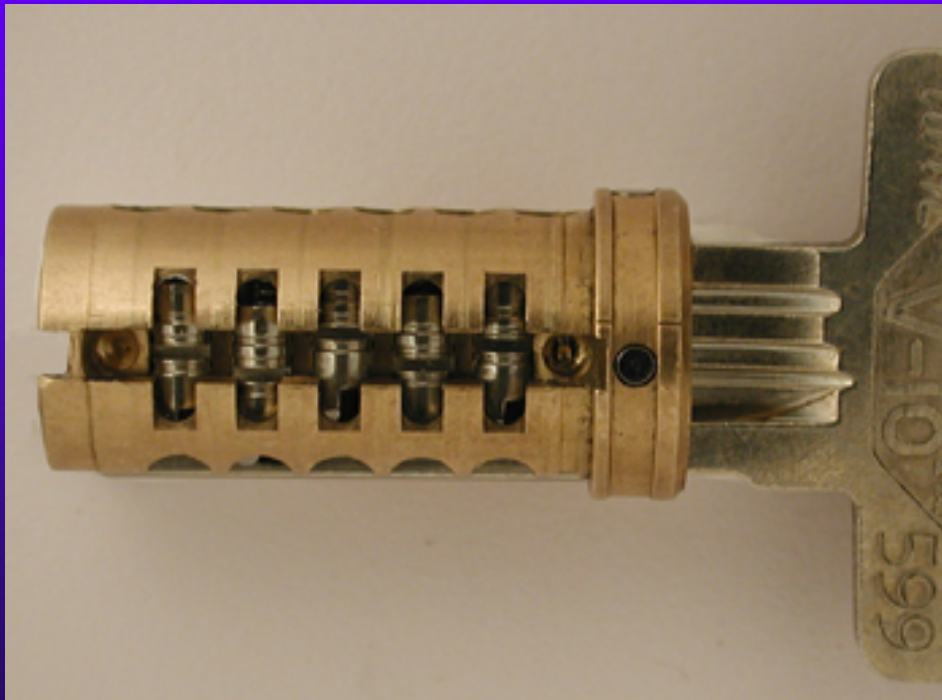


# ASSA V10





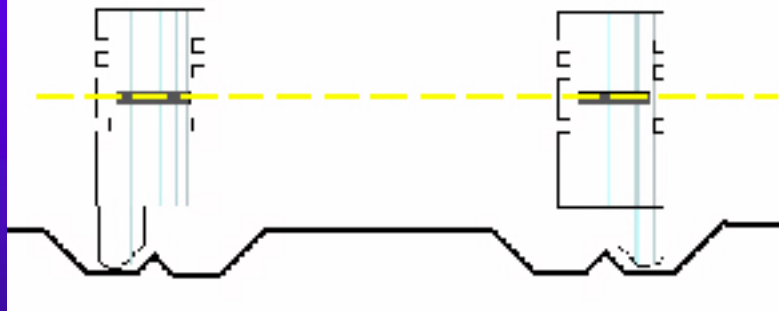
# ASSA V10 SIDEBAR DETAIL



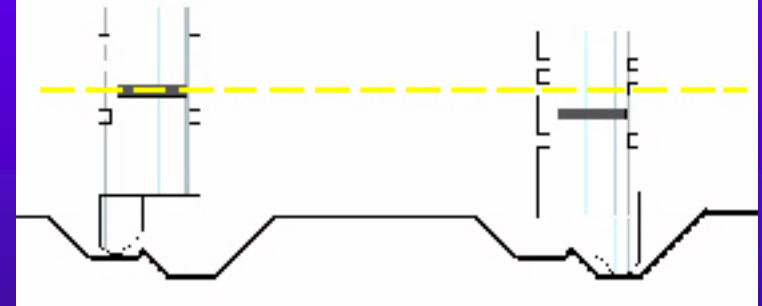
# ASSA Right and Left Pins



**V-10 balanced side cuts**

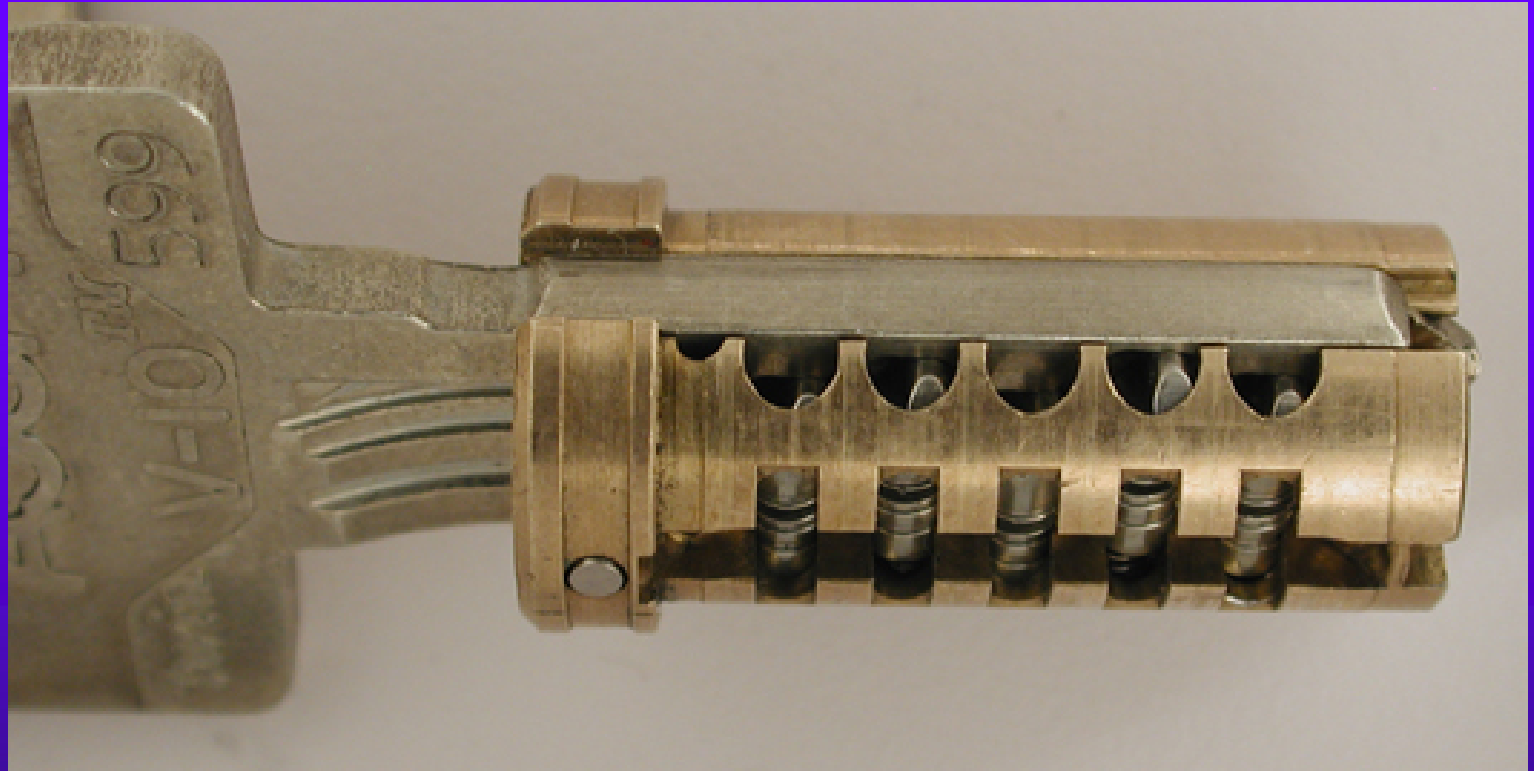


**V-10 unbalanced side cuts**





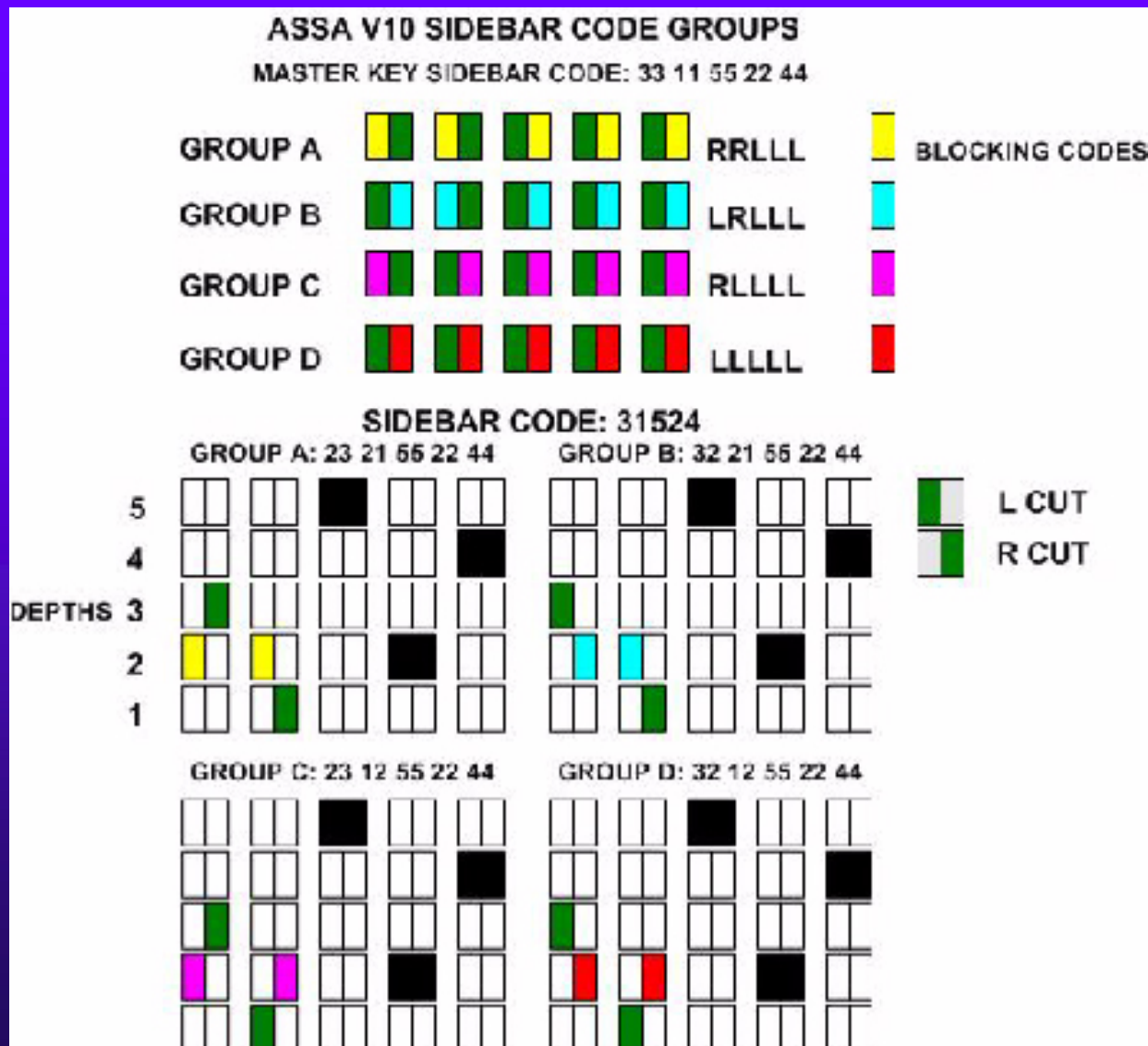
# ASSA LEFT-RIGHT CONTACT



# ASSA 32 Left-Right codes

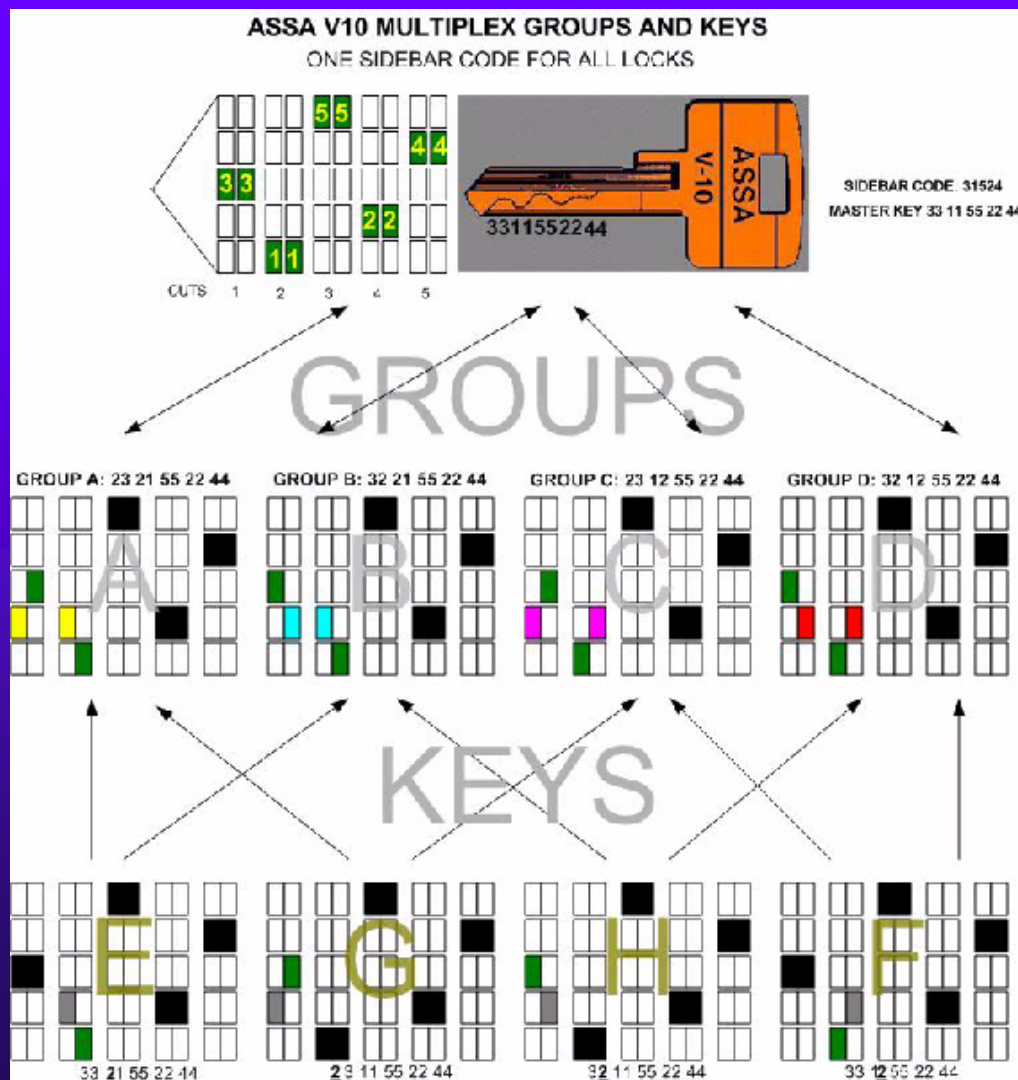


# ASSA: one sidebar code



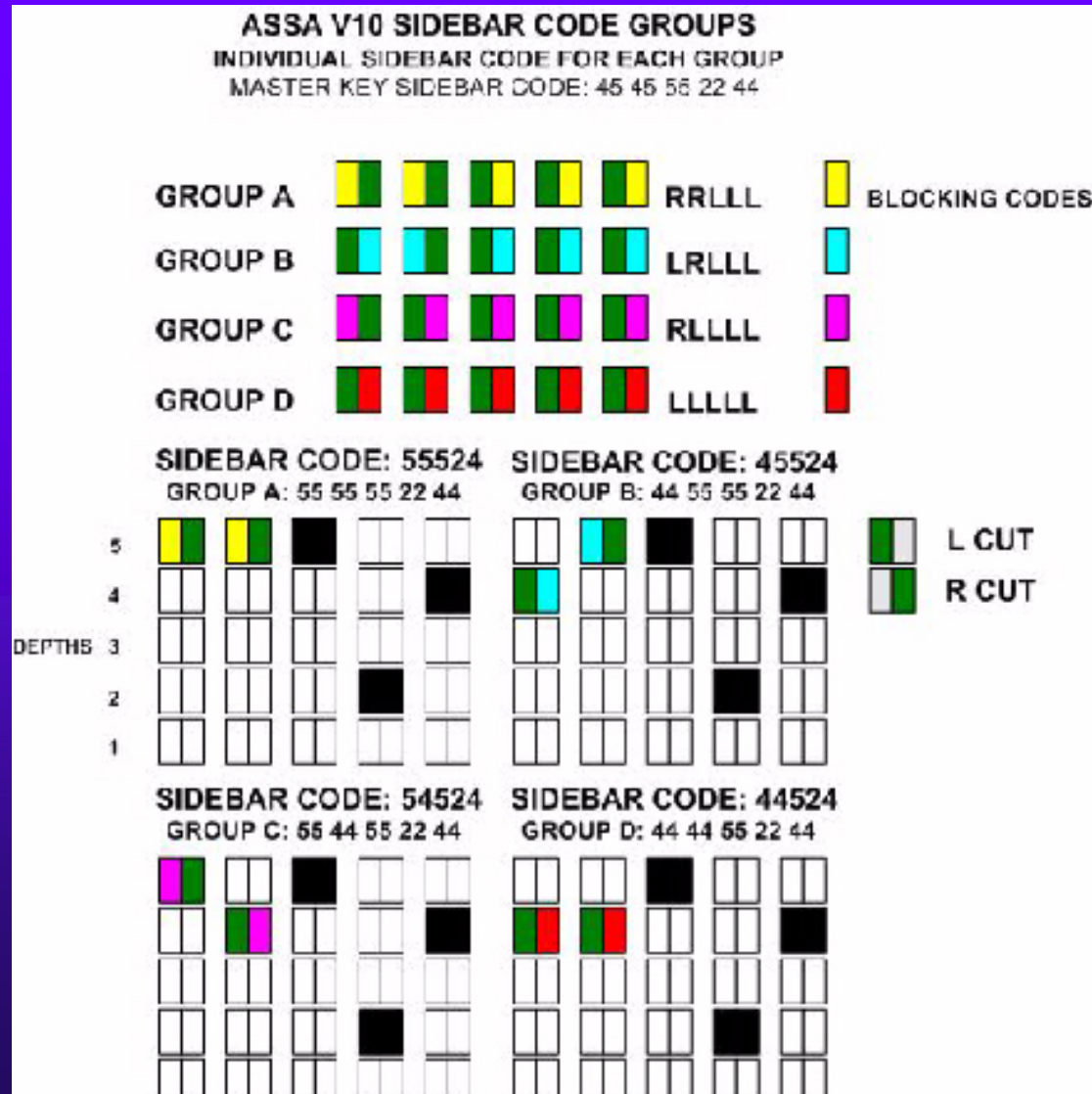
# ASSA: Keys and Groups

## One sidebar code

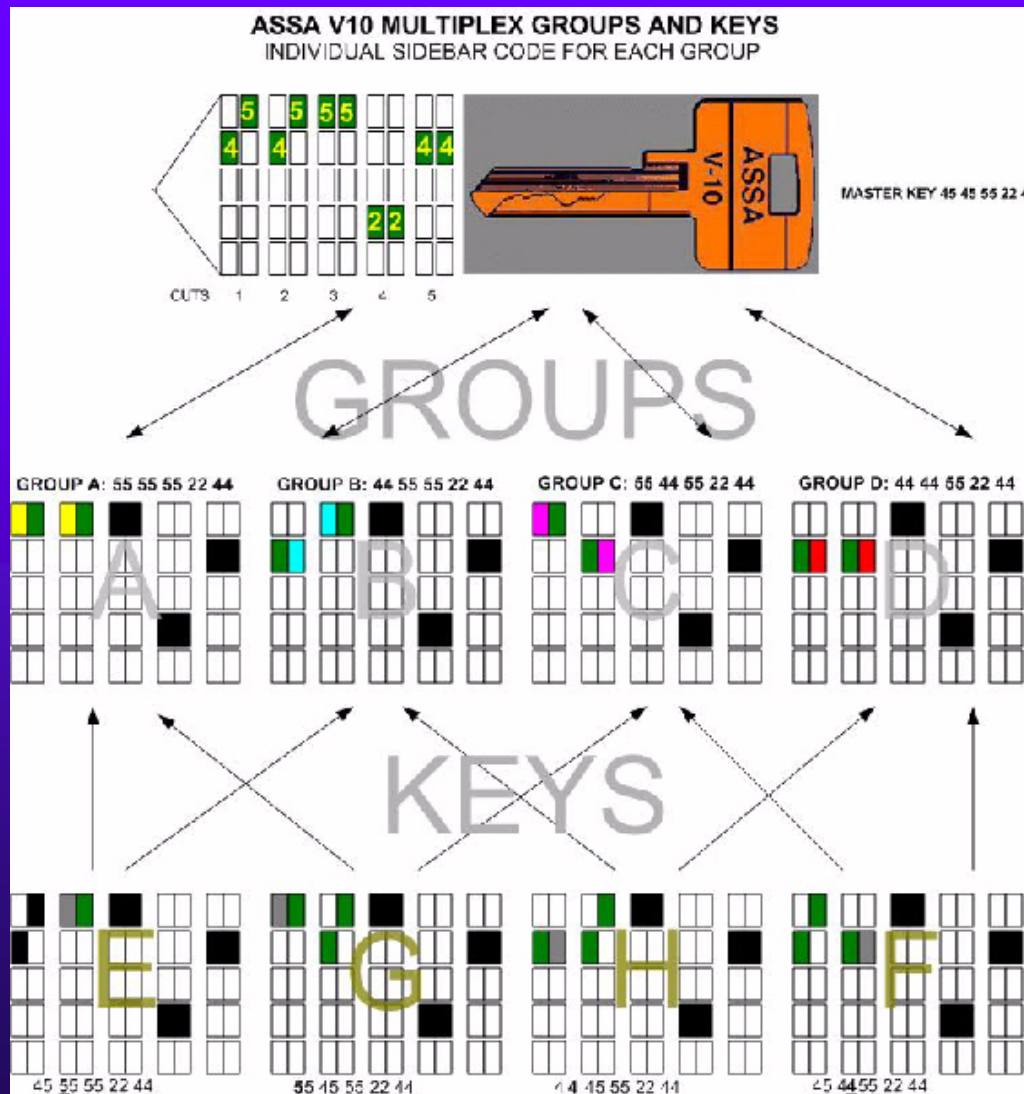




# ASSA: Individual sidebar codes



# ASSA: Keys and Groups for Individual Sidebar Codes





# ASSA v. MEDECO

- ◆ Each system offers enhanced security
- ◆ Each provides an increased number of differs
- ◆ Greater resistance against extrapolation
- ◆ Assa has more theoretical differs but may be easier to reverse engineer and obtain vital system information;
- ◆ Medeco routinely implements multiple sidebar coding within large systems; Assa does not.

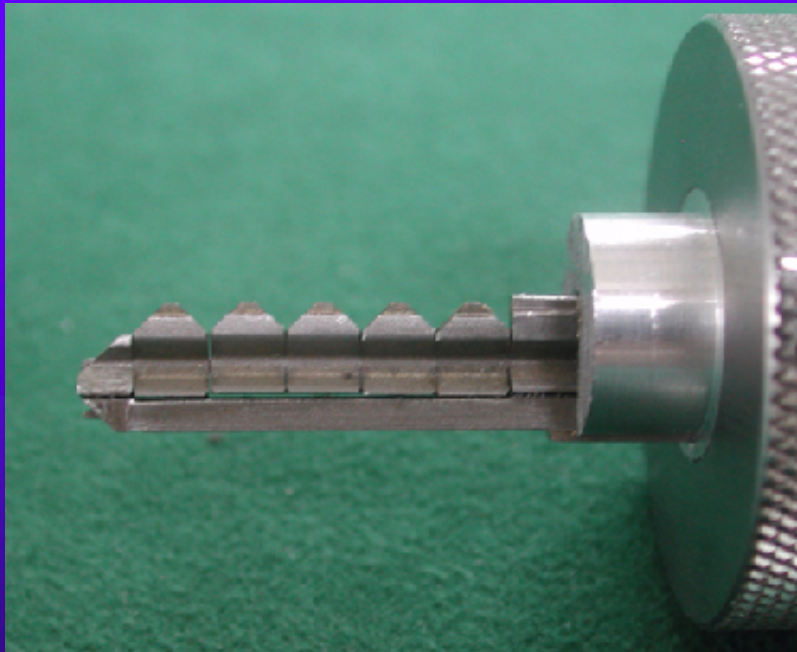




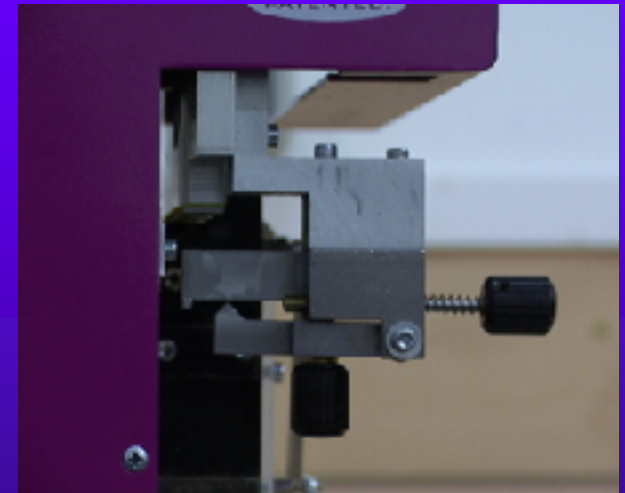
# EXTRAPOLATION: SPECIAL TOOLS AND TECHNIQUES

- ◆ Easy entrie profile milling machine
- ◆ John Falle pin lock decoder/pin-cam system
- ◆ Pack-a-punch
- ◆ HPC 1200

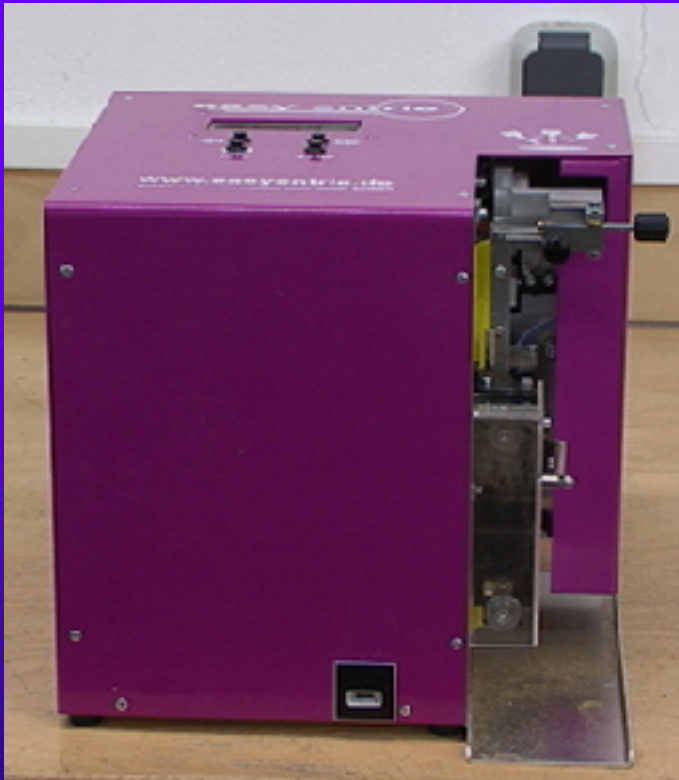
# FALLE PIN LOCK DECODING AND KEY GENERATION



# EASY ENTRIE

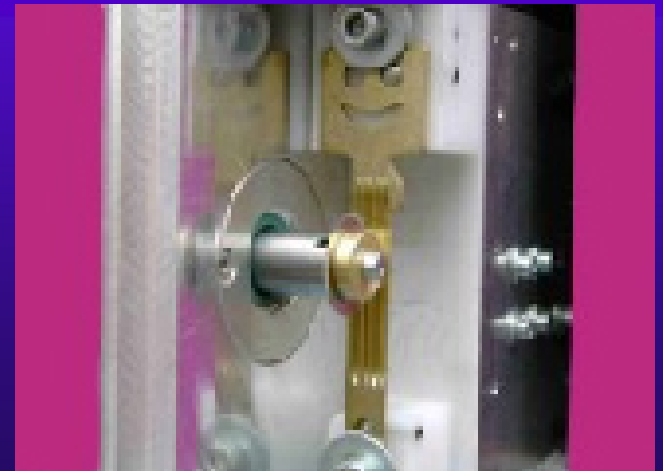
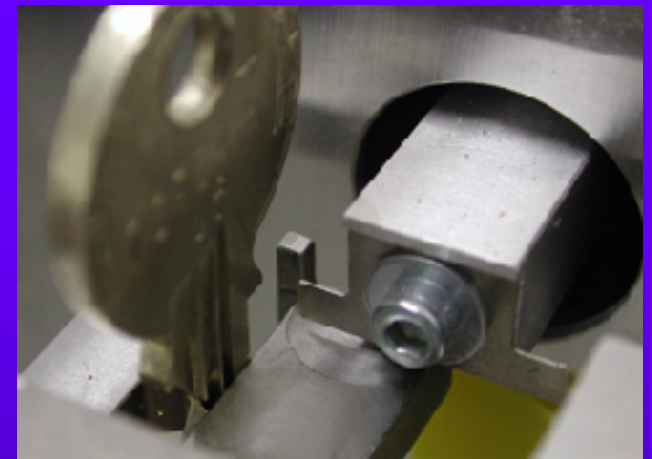
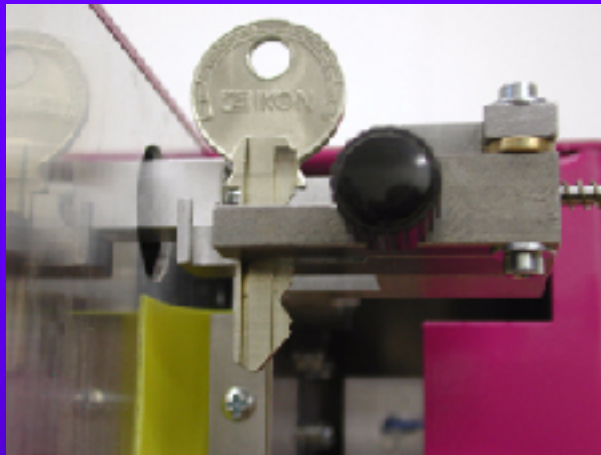


# EASY ENTRIE PROFILE MILLING MACHINE

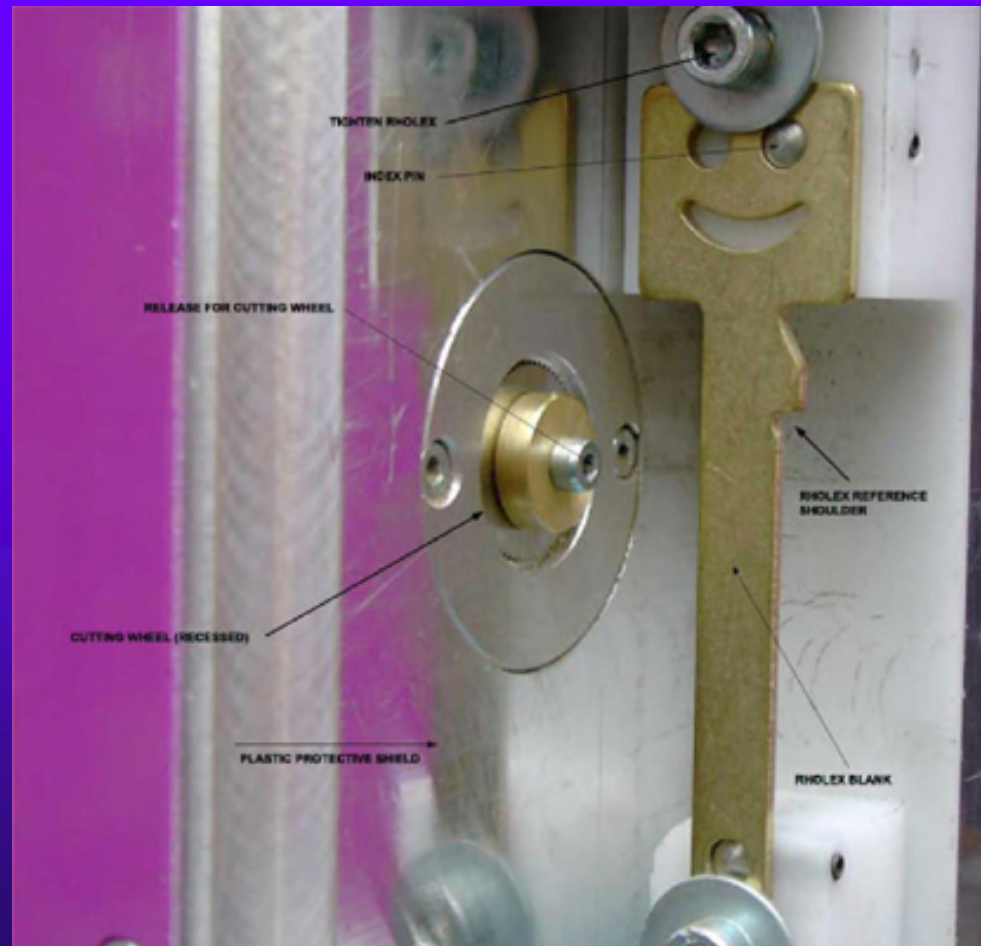




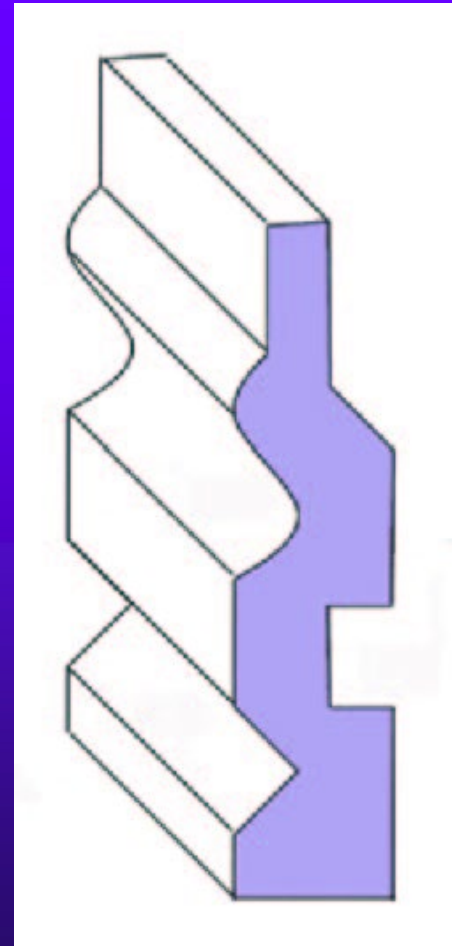
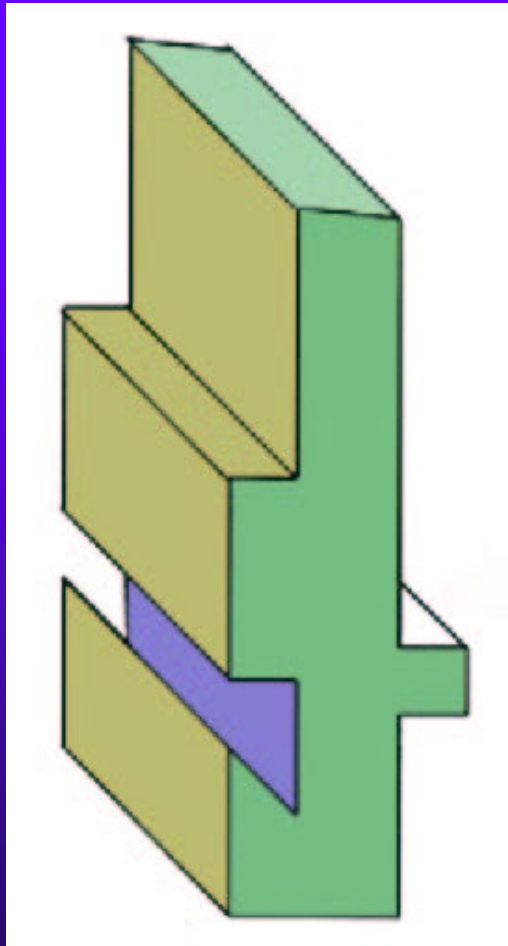
# EASY ENTIRE COMPONENTS



# Easy Entry Profile Milling

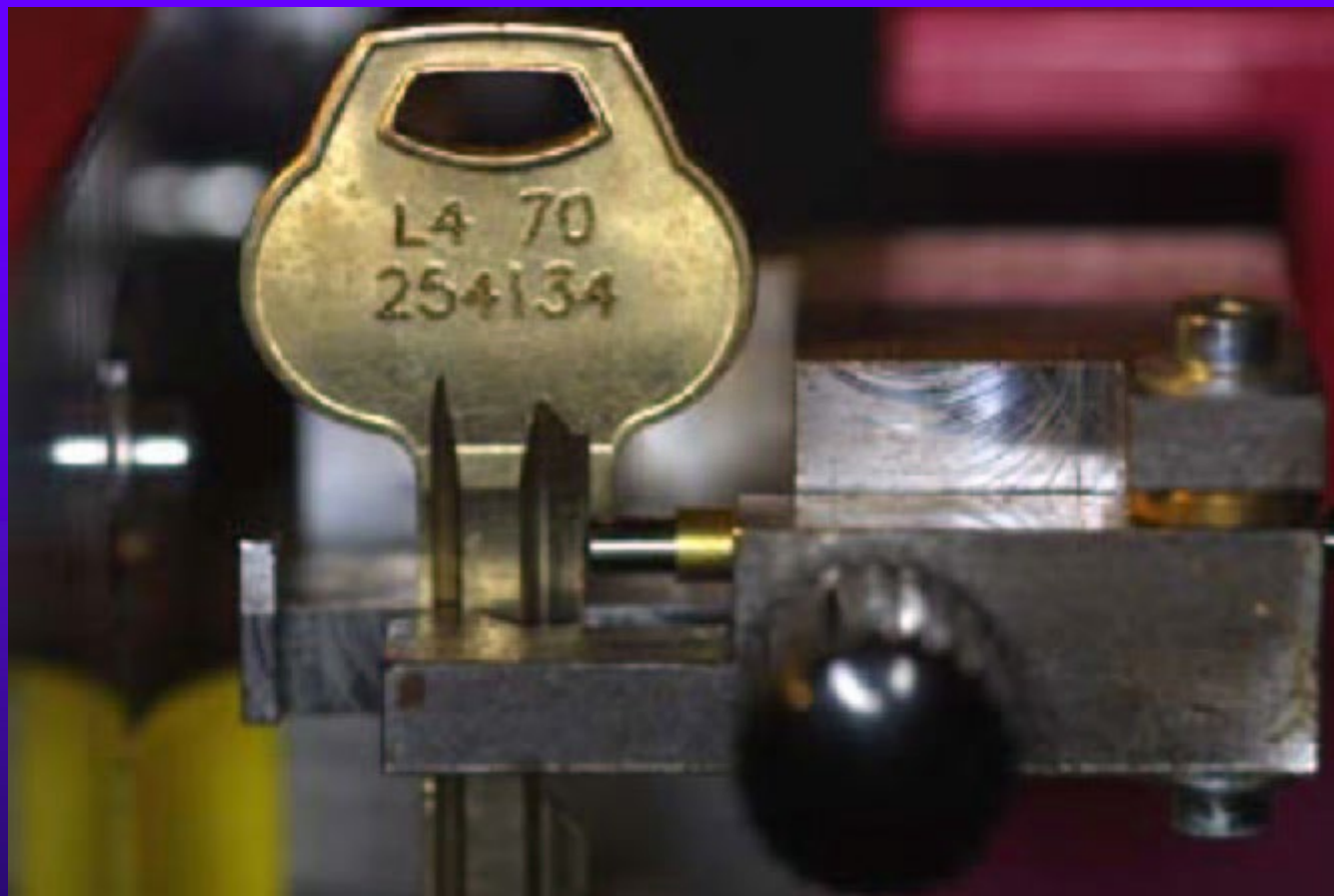


# Profile Measurement

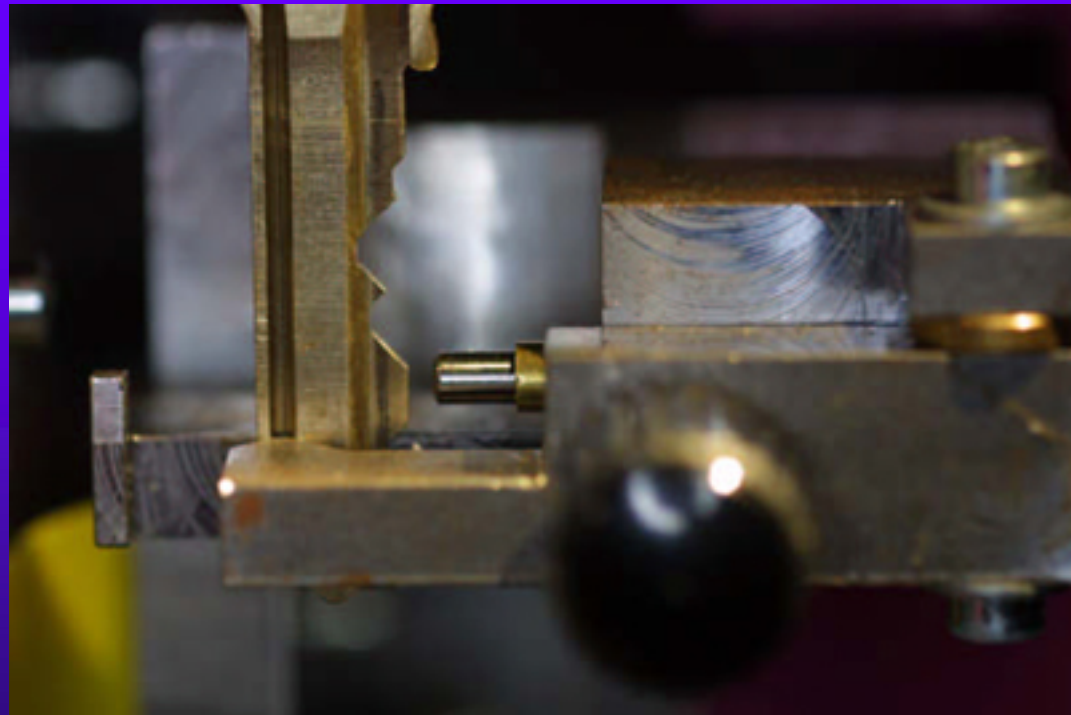




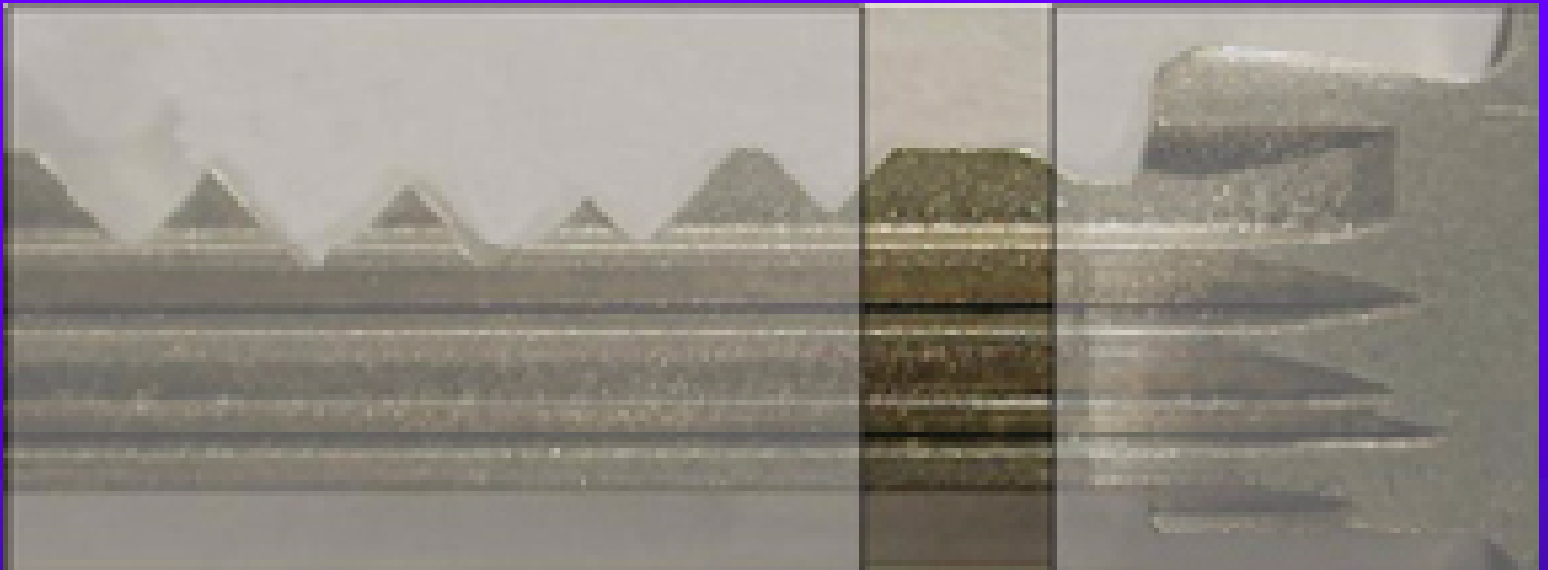
# Measurement of Blade



Cut key made into blank key



# Change key to Blank key



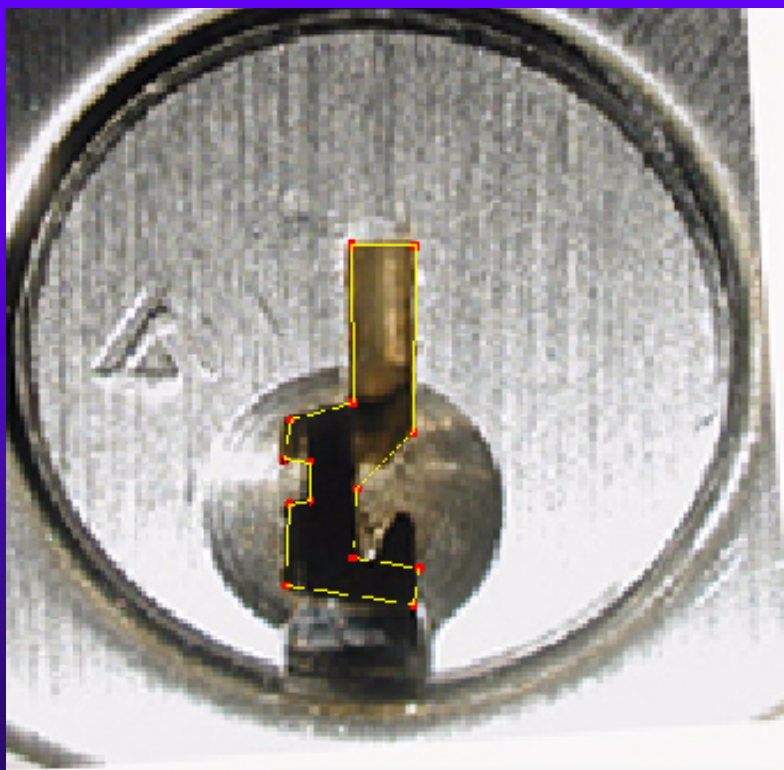
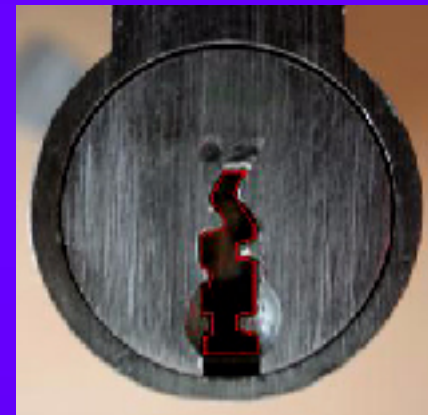
# EASY ENTRY KEYS







# EASY ENTRY PC



## Photo Profile

Diameter reference circle:

17mm Profilcylinder Ausser (Standard)

4.25 mm

Load photo...

Easy Entry

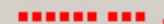
Drawing of the Profile is ready

Takes on the drawn Profile

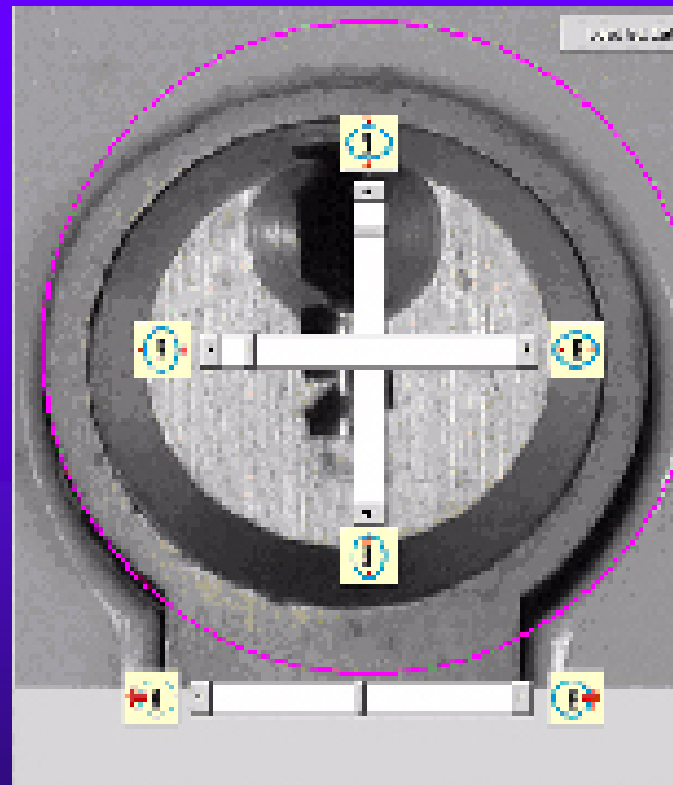
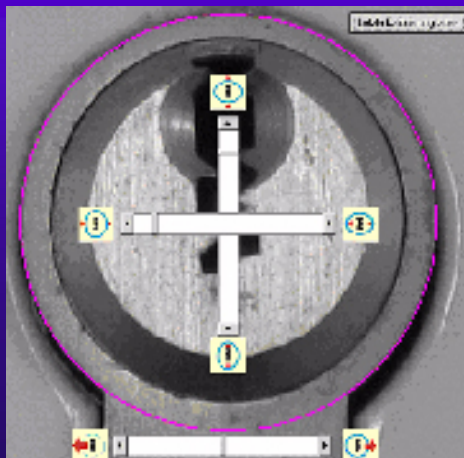
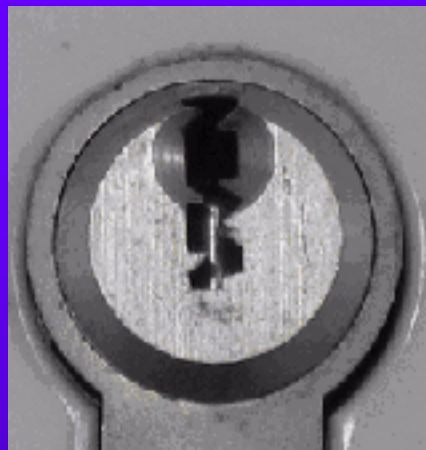
Profile is ready. Please click at  
> Takes on the drawn Profile

Move the drawing points

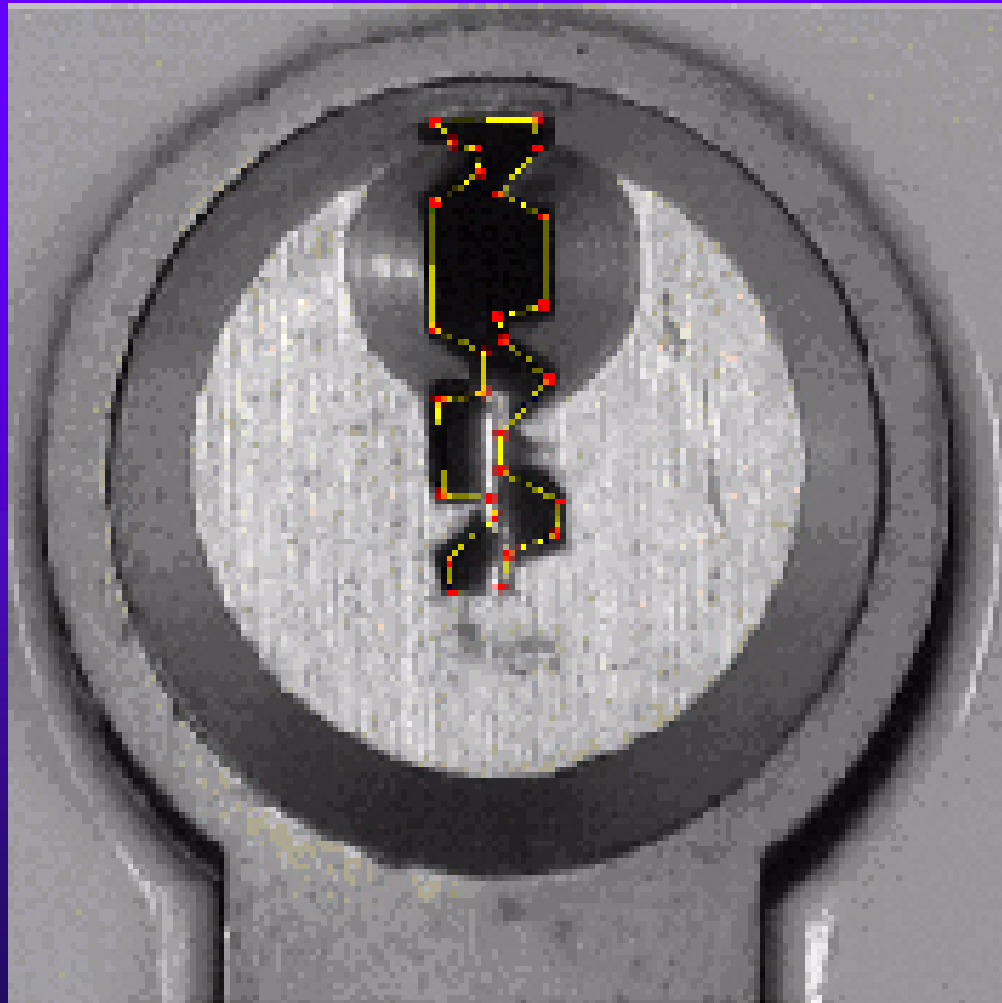
Cancel



# EASY ENTRY PC

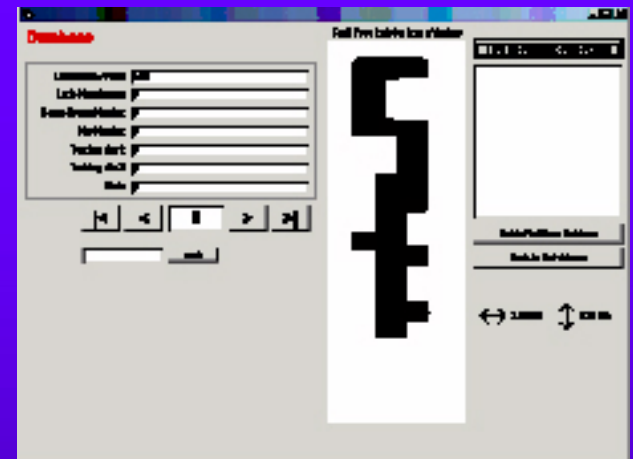
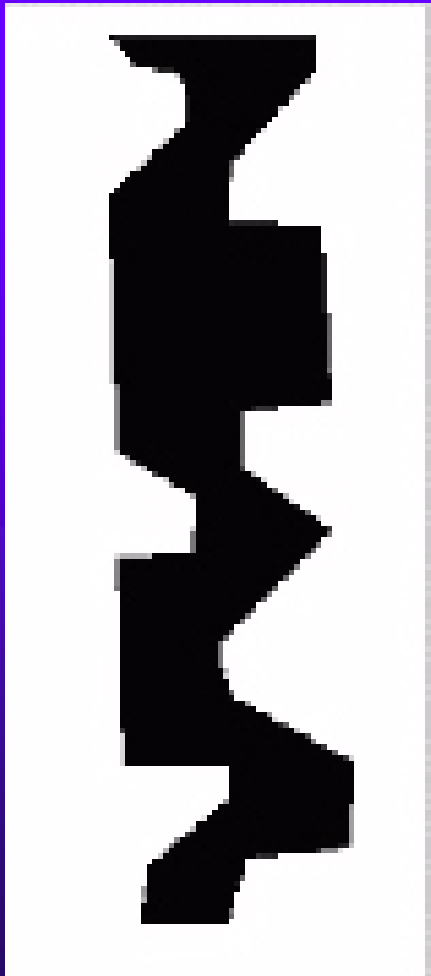


# EASY ENTRIE DRAW MODE

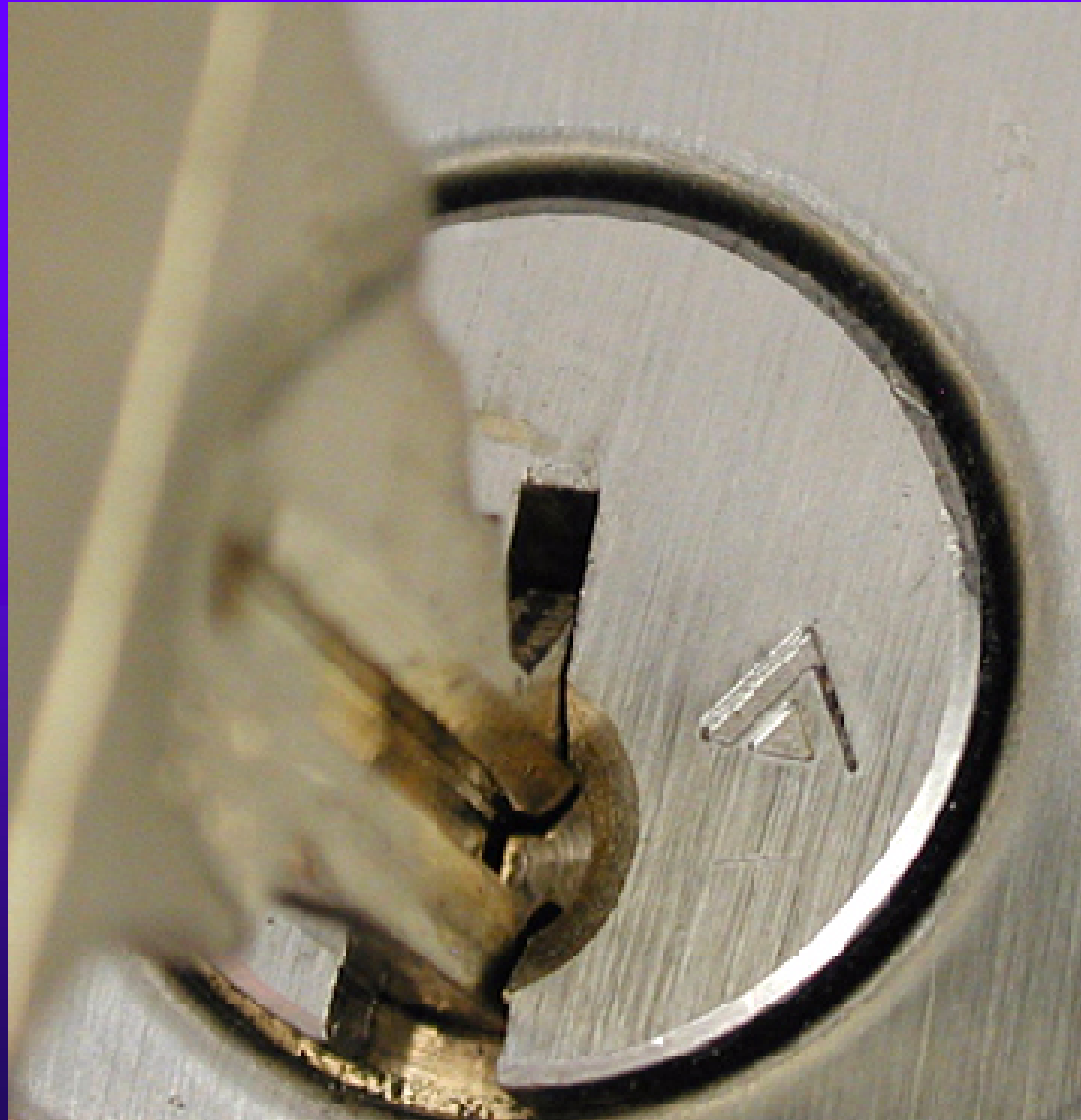




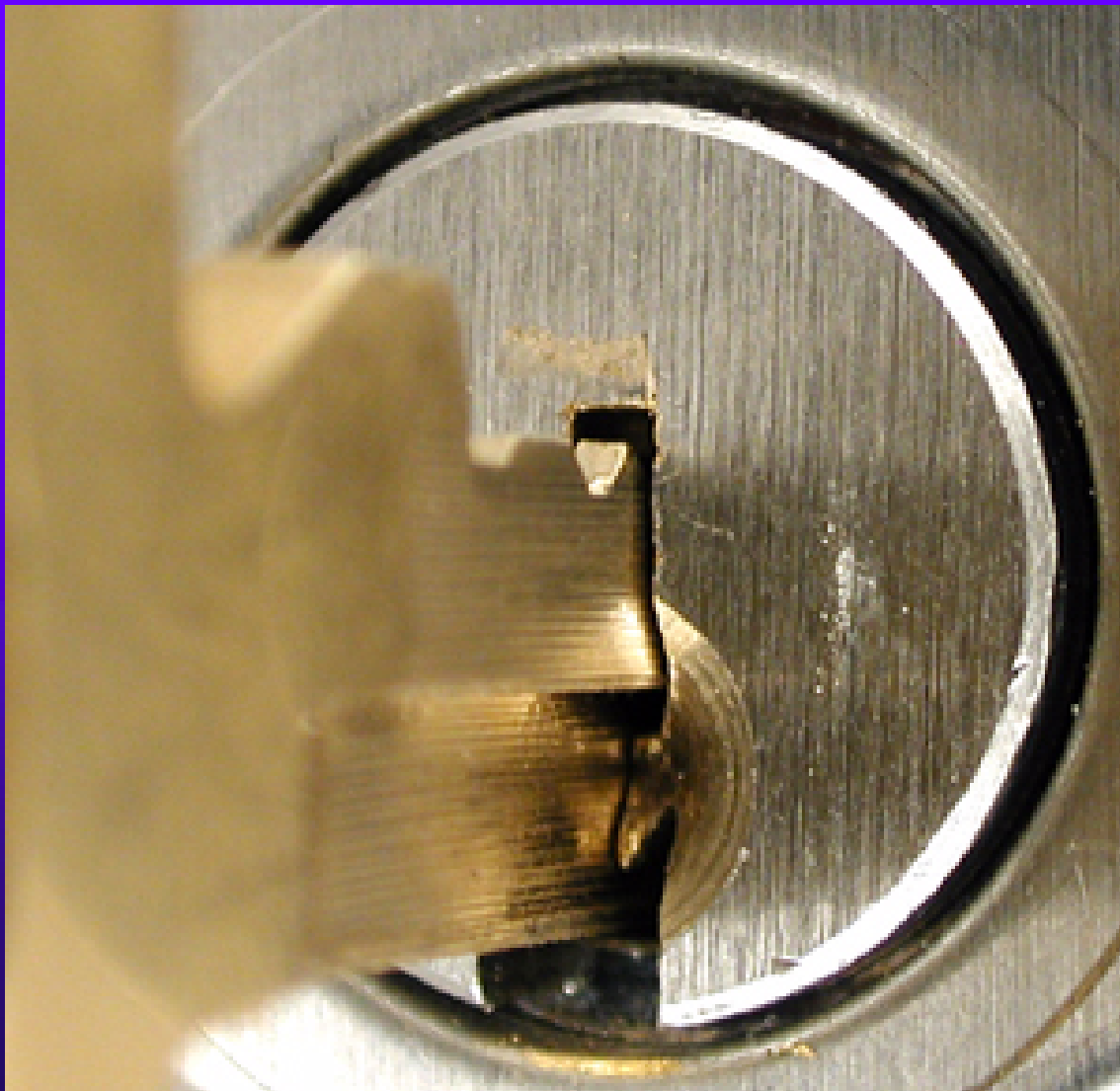
# MODIFY PROFILE



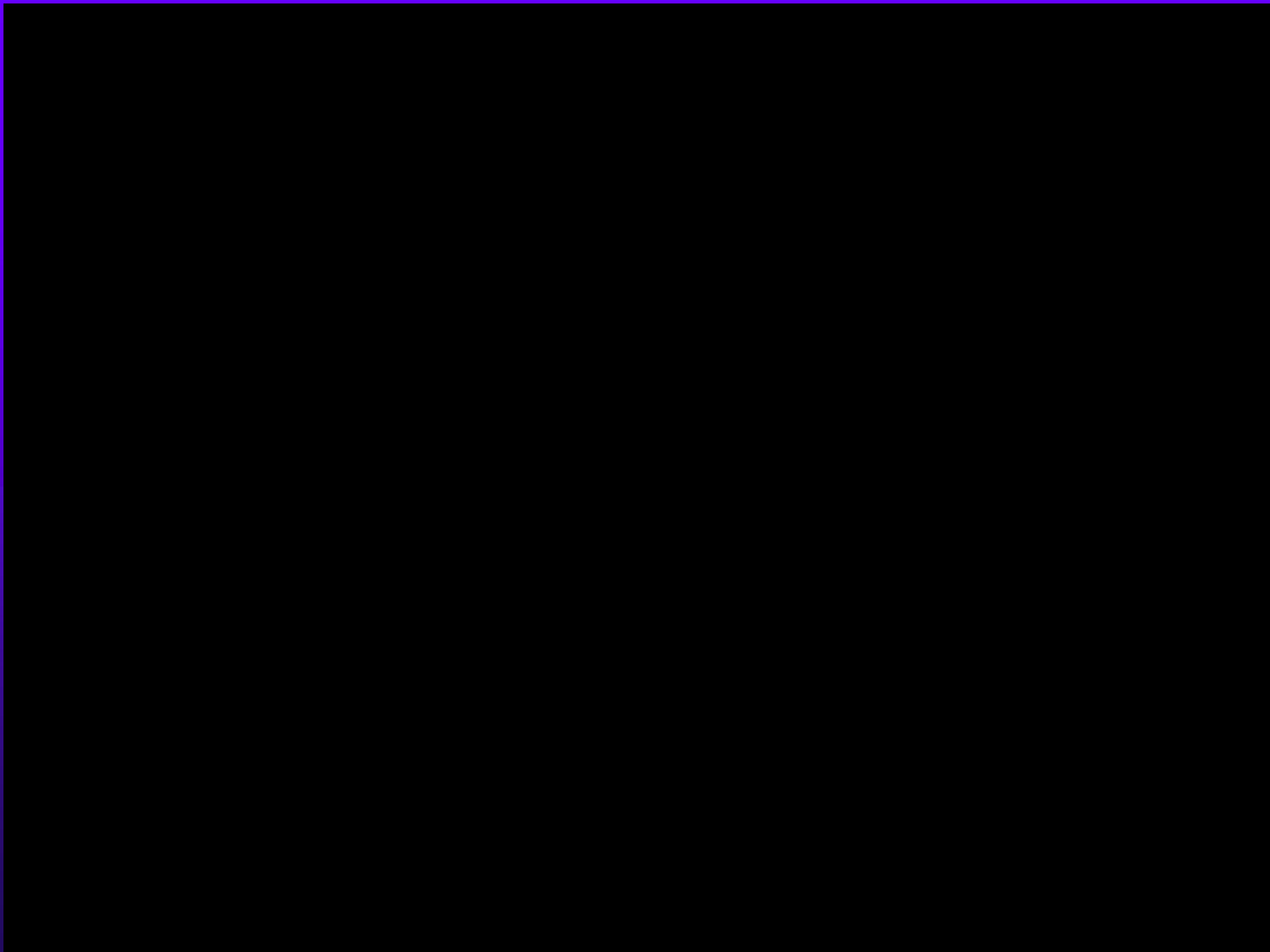
# Original Profile: Everest



# Modified Profile: Everest



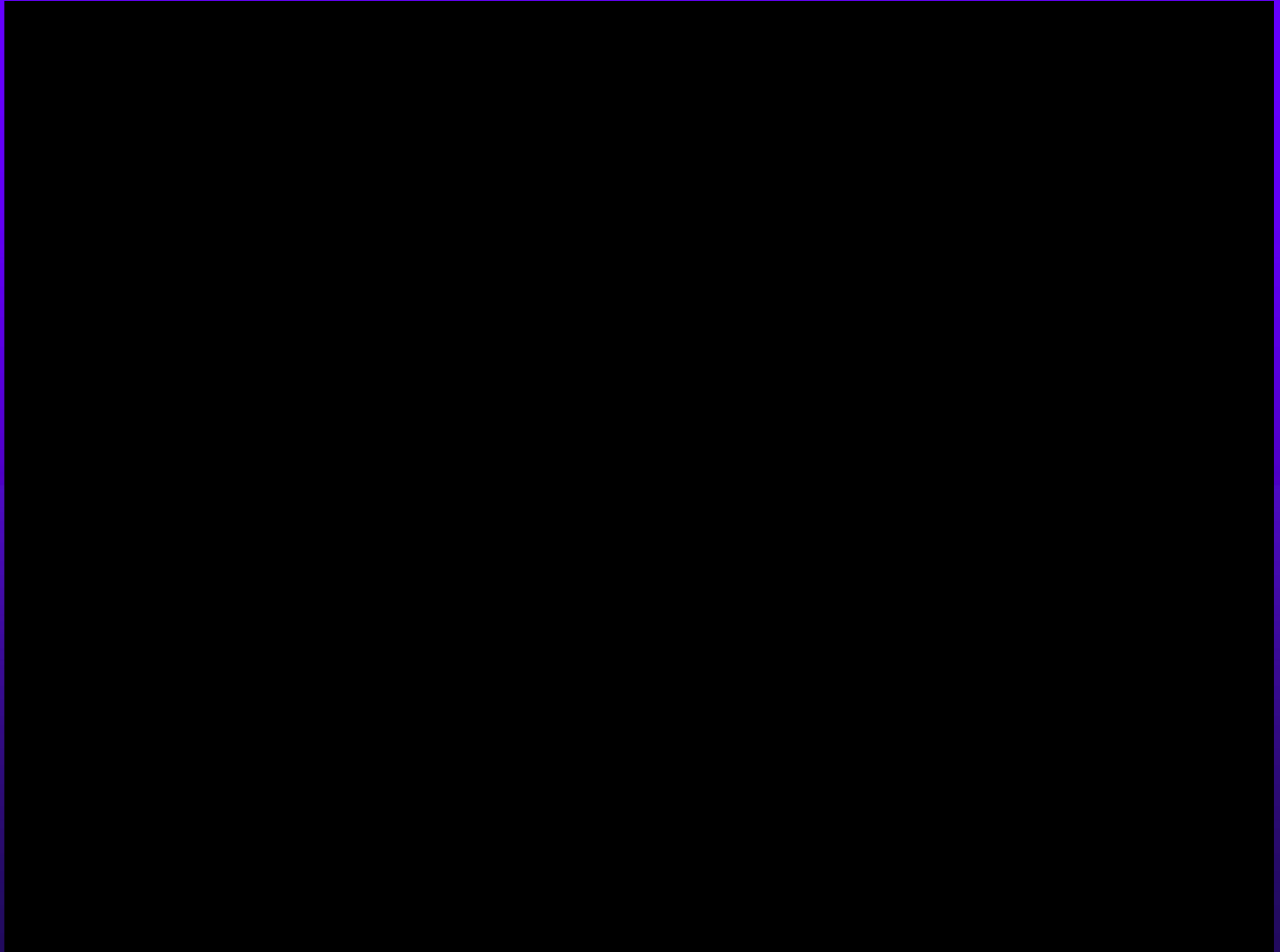
# EASY ENTRIE DEMONSTRATION



# MATT BLAZE ON EXTRAPOLATION



# HARRY SHER ON DECODING THE TMK AND SECURITY







# References

- ◆ M. Blaze. “Rights Amplification in Master-Keyed Mechanical Locks.” *to appear*. 2002.  
<http://www.crypto.com/mk.pdf>
- ◆ M. W. Tobias. *Locks, Safes and Security (2/e)*. 2001 and LSS+
- ◆ B. B. Edwards. *Master Keying by the Numbers (2/e)*. 1997.