Mul-T-Lock: Design and Security

by datagram, 2009-2012

1. Introduction

Hello, I'm datagram, I run www.lockpickingforensics.com and www.lockwiki.com. I chose to write about Mul-T-Lock because they are interesting and (mostly) unique on a technical level. Additionally, there are few references on how they work outside of marketing material, particularly for newer models. (Plus, Han Fey already did Abloy!)

This article analyzes Mul-T-Lock telescoping pin-tumbler systems throughout the company's nearly forty year history. We'll also look at security; attacks on the various Mul-T-Lock models and how the company has dealt with these problems. Finally, there are several appendices that provide keying, coding, and patent references for Mul-T-Lock systems.

I can be reached at datagram.locks@gmail.com. See http://www.lockpickingforensics.com/ for more contact information. Corrections, additions, comments, and criticism are all welcome.

Note: While I know more than most about Mul-T-Lock systems there are many areas where I could use your expertise. I've done my best to note these places; please contact me if you can help! All contributors will be properly credited unless anonymity is preferred.

2. History of Mul-T-Lock

Mul-T-Lock is an Israeli lock manufacturer founded in 1973 by Avraham Bachri and Moshe Dolev. The motivation behind Mul-T-Lock began in 1972 when a customer asked a locksmith to install “four extra locks for her front door.” After installing the locks the locksmith consulted with a friend and the two (Bachri and Dolev) designed a multi-point locking system. They went on to form a company around their system, eventually becoming the aptly named “Mul-T” Lock. The company gained international popularity over the next thirty years, designing and patenting a multitude of locking systems. Mul-T-Lock is currently one of the most recognized names in security. Their systems are used in a wide variety of high security installations, including many prisons. Mul-T-Lock was purchased by the ASSA-ABLOY group in 2000.

Though they hold patents for various locking mechanisms, Mul-T-Lock are best known for their dimple pin-tumbler locks that feature telescoping pin pairs, also known as pin-in-pin. In a normal pin-tumbler, pin pairs have a driver and key pin which separate at the shear line to open the lock. A telescoping system uses two sets of pin pairs, one outer pair and one inner pair. The outer pin encases all but the tips of the bottom inner pin pair. Both inner and outer tumblers must be properly aligned at the shear line to open the lock.

The original idea for a telescoping pin-tumbler dates as far back as 1897. Thorsten Rydberg's 1897 patent titled “Lock” describes a lock in which “*each tumbler consists of such a severed pin or bar (solid or hollow) surrounded by one, two, or more concentric tubes, severed and spring-actuated in the same manner as the pin, or it may be of only two or more concentric tubes made to slide in each other.*” Unfortunately, the patent images are not very clear, but the text clearly describes telescoping pins.

In 1914 an interesting telescoping pin-tumbler patent was granted to Christian Hansen of Davenport, Iowa. In Hansen's design, a double bitted pin-tumbler key is used to position telescoping pin pairs (Figure 2.1) on the top and bottom of the keyway. In his design there are inner pins, intermediate sleeves, and outer sleeves. One of Hansen's claims is the ability that the key can be withdrawn in either horizontal orientation, an interesting effect of the position of tumblers and an inverted key bitting. The negative effect of this claim is that number of key differs is drastically reduced for the sake of usability. Hansen provides a complex description of the telescoping pins:

> “*The radial inner pin 24 and the sleeves 26 and 28 of each tumbler, upon insertion of the key 14, are moved outwardly the proper distance so that their outer ends come into registration with the periphery of the key cylinder 9, whereby the latter may be turned.*”

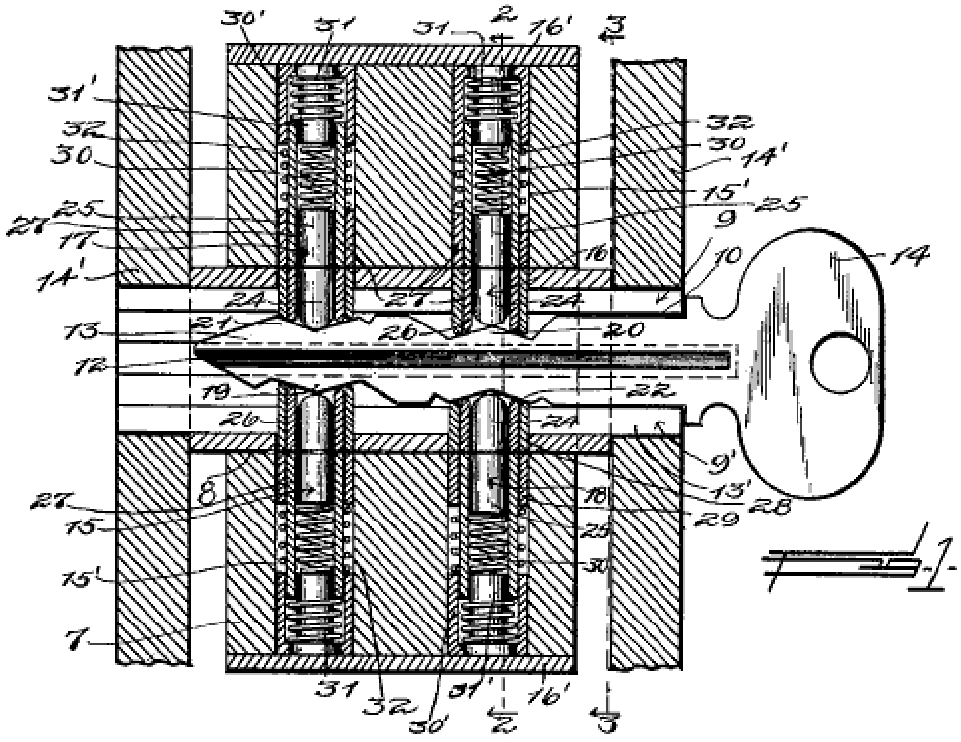


FIGURE 2.1: 1914, Patent images showing a dual-bitted pin-tumbler key with telescoping pins on the top and bottom of the key blade.

In 1935 Clarence L. Williams and Earl M. Simmons were issued a patent that describes a lock with components described as a "double interfitted pin type." The patent image (Figure 2.2) shows telescoping pins being used on a traditional pin-tumbler key on both the top and sides of the bitting area. The design of the telescoping pins in this patent most closely resemble early generations of Mul-T-Lock telescoping pins.

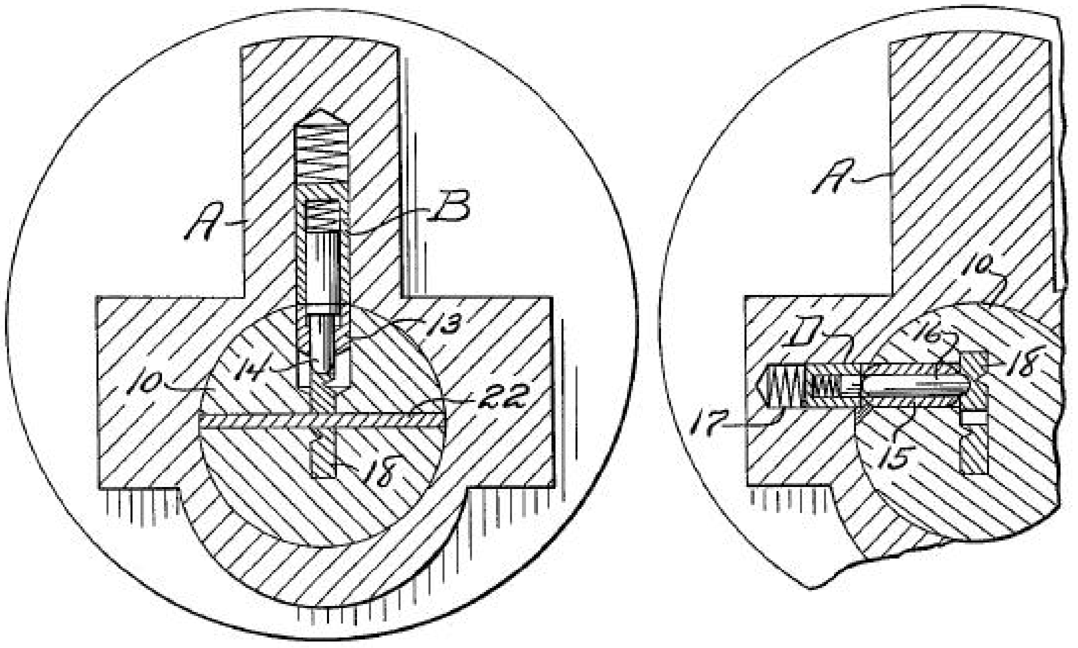


FIGURE 2.2: 1935, Patent images showing outer (13/15) and inner (14/16) telescoping pin-tumblers on the top and side of the keyway.

In 1977, Avraham Bachri and Moshe Dolev, founders of Mul-T-Lock, were granted a patent for a telescoping pin-tumbler lock. Unlike the 1935 version, this model has one row of telescoping pins and uses a horizontal keyway with dimple key. Another important addition was the inverted mushroom security pins and the use of a round mating surface between the pins, plug, and cylinder. This improves tolerances to enhance keying capabilities and pick resistance. Noach Eizen of Mul-T-Lock was granted a patent in 1987 for a similar telescoping pin lock.

The 1977 and 1987 patents are the basis for the Mul-T-Lock Classic model. The Classic began a rich history for Mul-T-Lock, the basic principles of which still exist in modern Mul-T-Lock designs. The next few sections will discuss the various Mul-T-Lock models, how they work, and varieties in their design.

3. Mul-T-Lock Classic

The original Mul-T-Lock telescoping design, patented in 1977, is dubbed the Classic. The Classic is a dimple lock featuring four or five telescoping pin stacks. The addition of telescoping pins does not change how a dimple pin-tumbler lock works, fundamentally. Pins must still be raised to the correct position; only now that includes both inner and outer pins. When all pins are correctly positioned at the shear line the plug can rotate. One important distinction is that inner and outer pins can be raised to different heights and a specially cut key is required to do so.

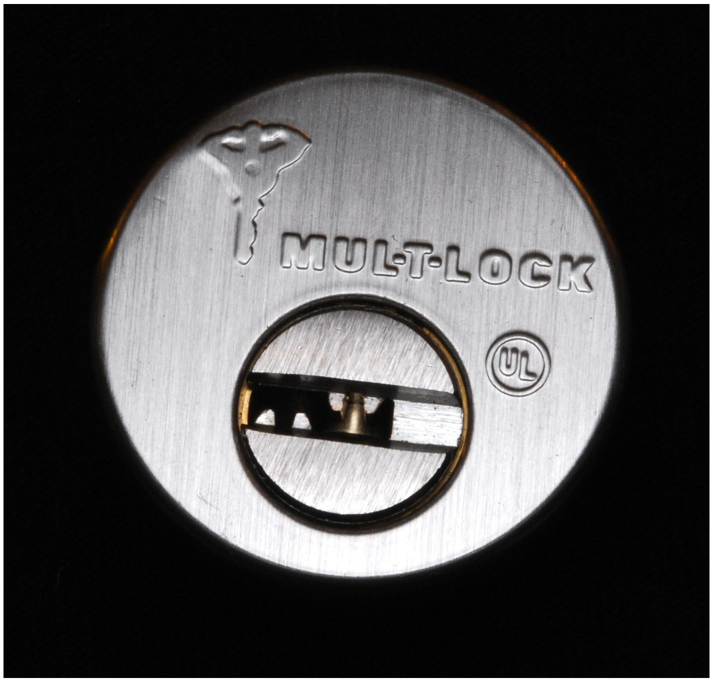


FIGURE 3.1: The Mul-T-Lock Classic, 006 keyway

Telescoping Systems

The Mul-T-Lock Classic is the first in a series of telescoping locks developed by Mul-T-Lock. From the outside it looks like a standard dimple lock (Figure 3.2). When disassembled we see a unique look to both the pin-tumblers and the plug. When the correct key is used both inner and outer pin-tumblers are aligned at the shear line (Figure 3.3). When an incorrect key is used inner and outer pairs are misaligned, causing the shear line to be blocked by one or both sets of pins. This design is the basis for all Mul-T-Lock telescoping systems.

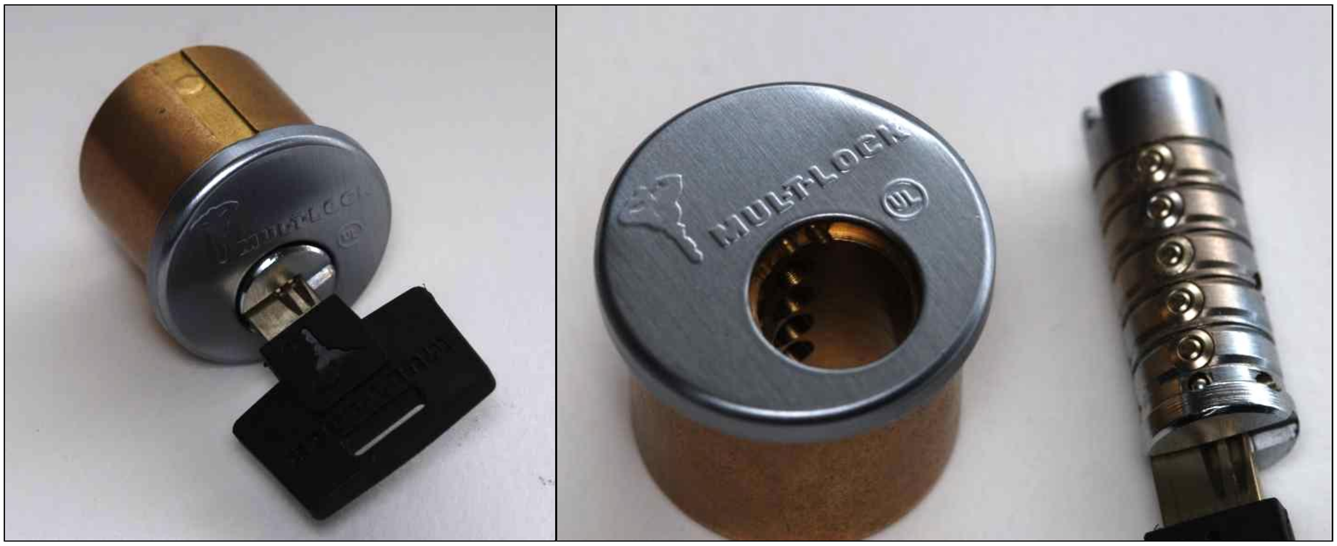


FIGURE 3.2: A Mul-T-Lock Classic rim cylinder assembled (left) and disassembled.

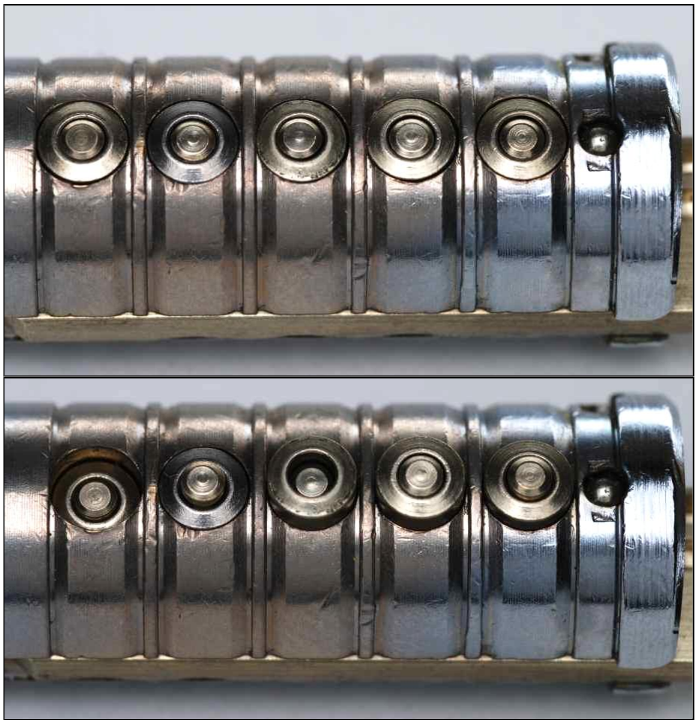
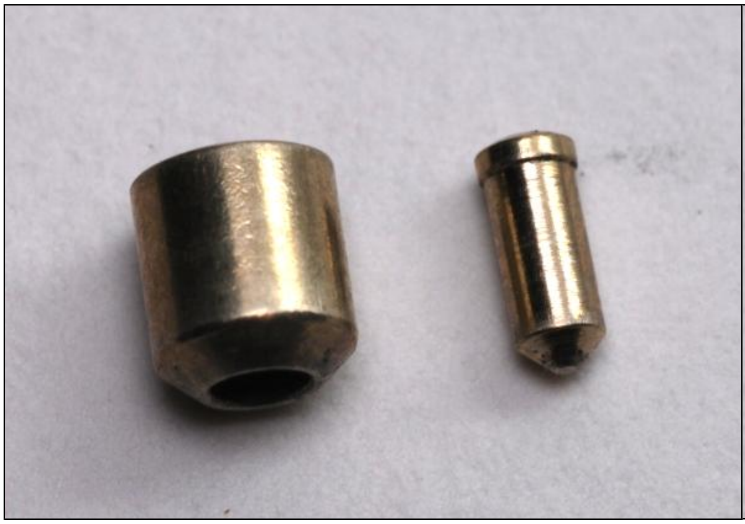


FIGURE 3.3: The Mul-T-Lock Classic when the correct (top) and incorrect (bottom) keys are used.

Telescoping Pins



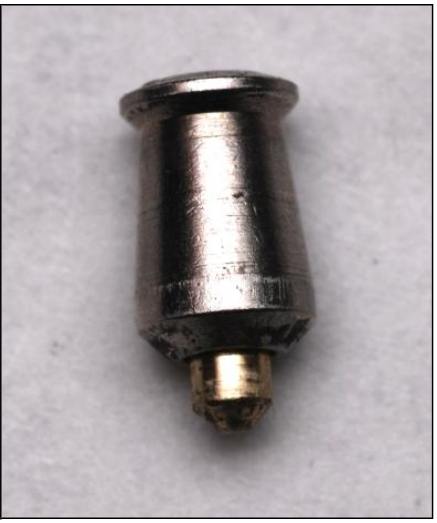


FIGURE 3.4 (Left): Standard Classic inner and outer key pins
FIGURE 3.5 (Right): An inverted mushroom outer key pin

The key pins consist of an inner and outer pin pair (Figure 3.4). The inner pin is spooled to prevent it from falling through the outer pin, but it also acts as a mild anti-picking mechanism. Outer key pins are generally standard, though there are variations that resemble an inverted mushroom that provide resistance to lockpicking and impressioning attacks (Figure 3.5).

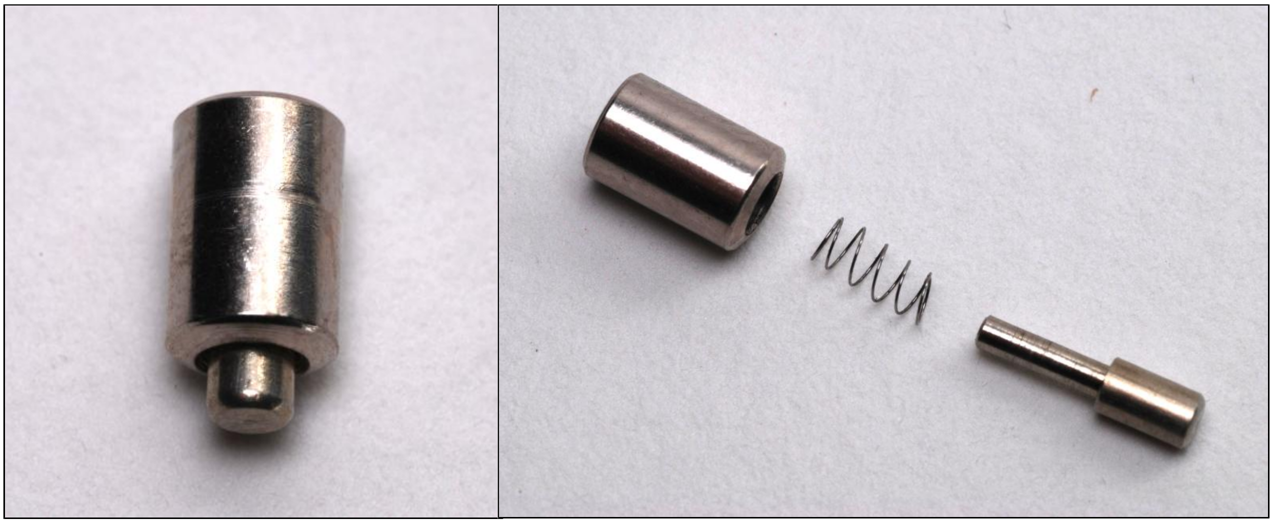


FIGURE 3.6: Assembled and exploded views of standard Classic driver pins

The driver pins are a three piece assembly of outer pin, inner pin, and inner spring (Figure 3.6). The inner spring pushes down the inner pin stack, and the design of the driver pins allows the inner pin to escape the driver pin, but only partially. This design is a result of a serious vulnerability known as the “Michaud Attack,” discussed further in *Section 8; Security Analysis*.

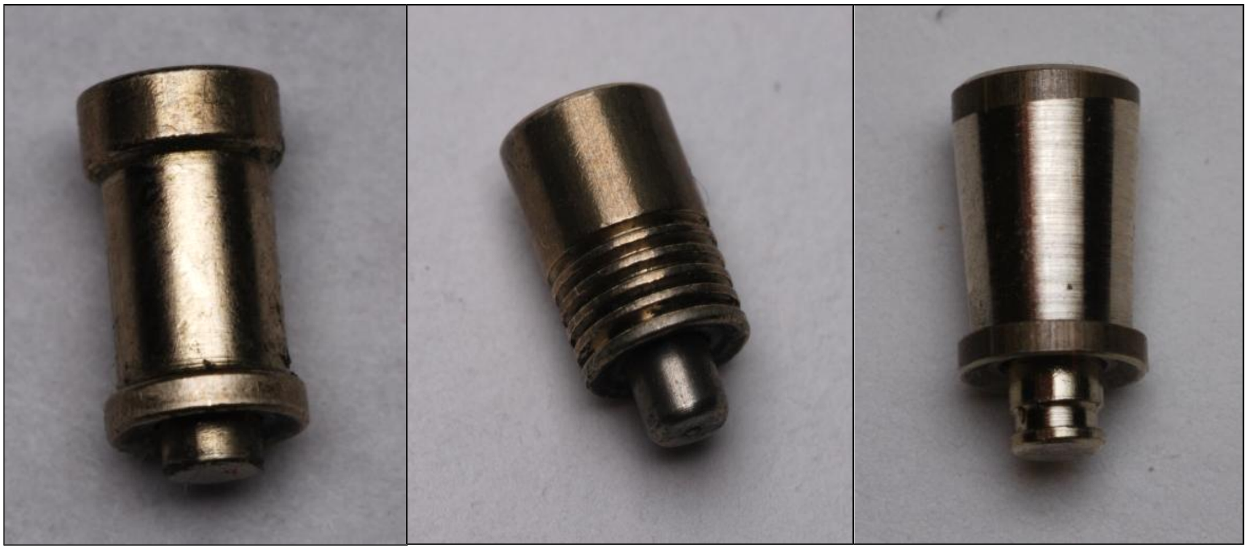


FIGURE 3.7: Spooled, serrated, and mushroom driver pins. Also note the serrated inner pin (right).

Outer driver pins have several security designs, including: spooled, mushroom, and serrated (Figure 3.7). Serrated are the most popular security pins in Mul-T-Lock's telescoping models — their traditional dimple locks favor spooled pins. Mul-T-Lock is interesting because they used various designs; most companies stick with one. Inner driver pins can also be lightly spooled (3.7, right) and combined with key pins that have internal counter-milling for additional pick resistance. A traditional spring is used above the driver pins to push *all* pin stacks down.

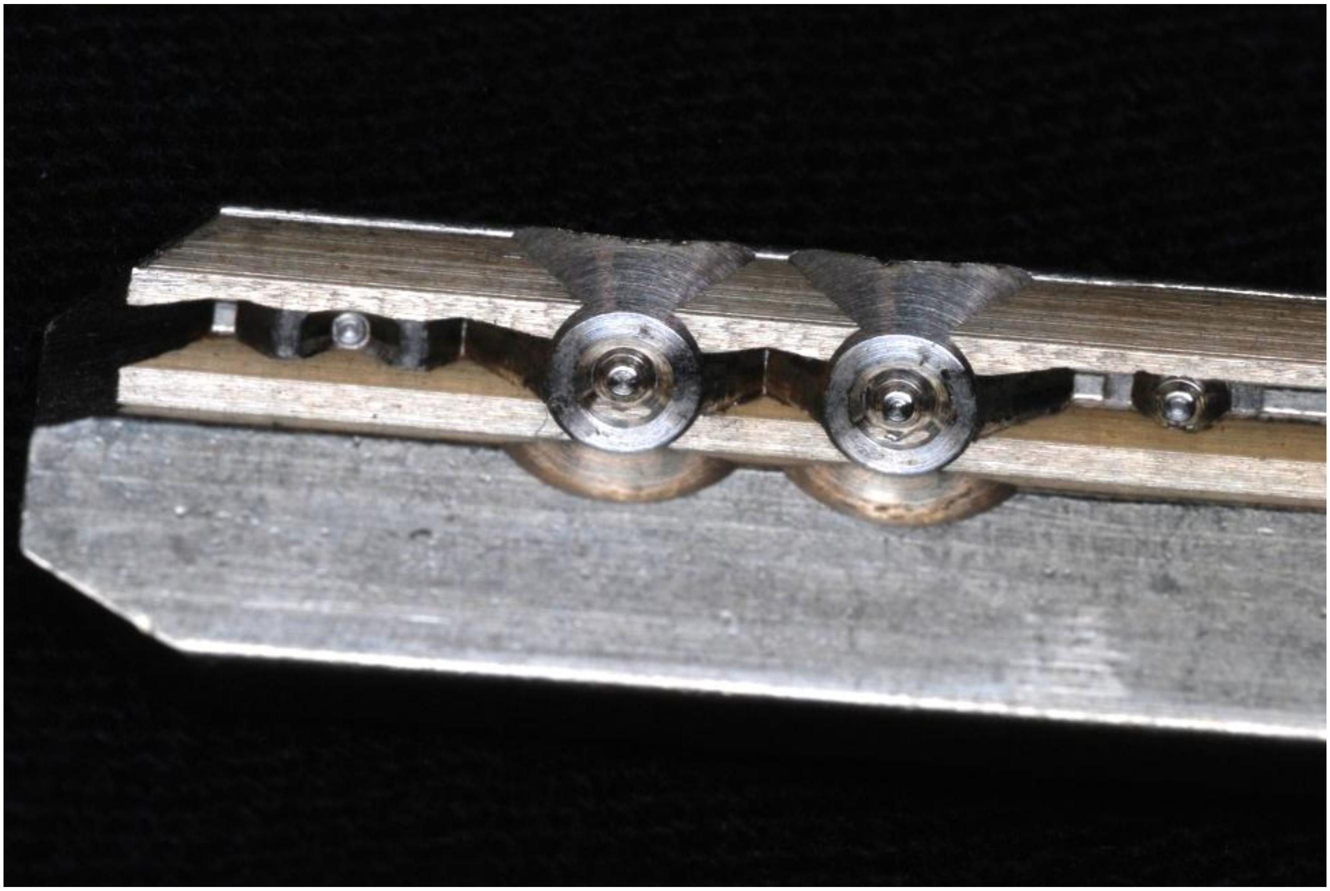


FIGURE 3.8: Bitting of a Mul-T-Lock Classic key, keyway 006C.
Notice the concentric cuts used to position each telescoping pin.

Keying Specifications

Unlike traditional dimple pin-tumblers, a specially cut key allows telescoping pins to be raised to different heights. Key cuts are a combination of two concentric rings, one each for inner and outer pins (Figure 3.8). This makes key duplication more difficult, slightly increasing key security. Of course this only defends against casual duplication; a determined attacker can easily reproduce a Classic key.

All Classic keys are tip stopped, meaning further insertion is prevented by the tip of the key contacting the cam (back) of the lock. This is interesting because it means that all Classic keys, whether they be for a 4 or 5 pin lock, can be bitted for 5 pins. When used in a 4 pin lock, the first four cuts manipulate tumblers and the fifth is unused. Classic keys are also “convenience” keys, meaning the key can be inserted in either orientation for proper operation.

Most Classic keys are sized alike but there are some that use a shorter key (cuts are still properly spaced). These are pretty rare; I have only run across a few in the many Classic keys I own or have had access to.

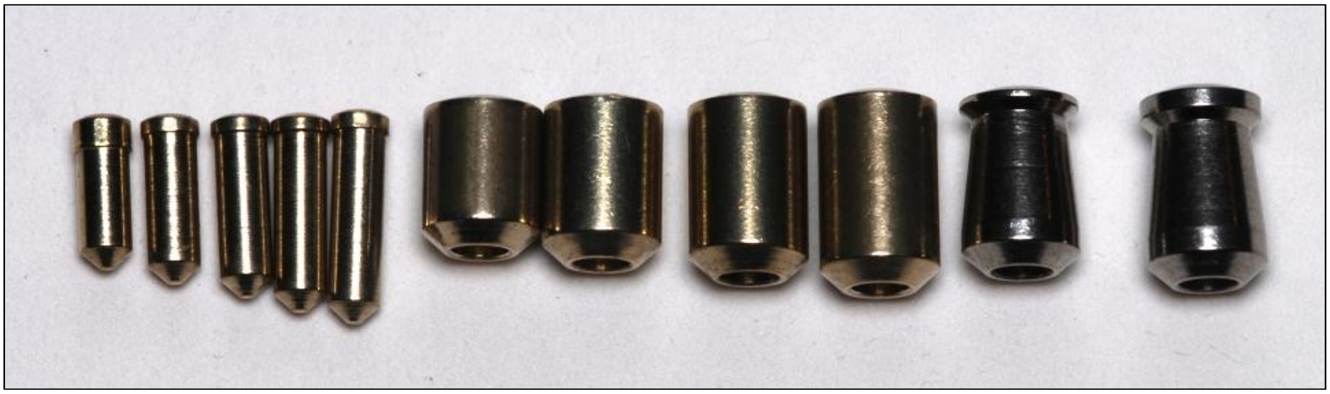


FIGURE 3.9: Classic key pins (all). Notice the difference in lips on the mushroom pins.

There are four depths available for outer pins, designated A-D, with D being the largest. Mushroom key pins can be used but only as C and D pins. There are five depths available for inner pins, designated 1-5, with 5 being the largest (Figure 3.9). Full key and pinning specifications are listed in *Appendix A: Keying Specifications*.

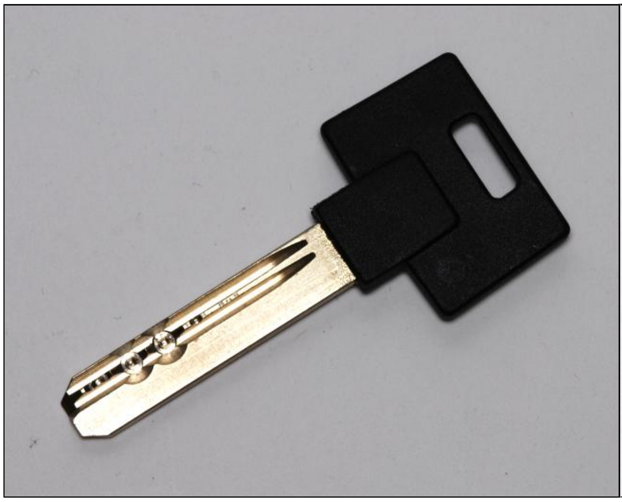
There is no Maximum Adjacent Cut Specification (MACS) for the outer pins, but between inner and outer pins there are a few restrictions:

- With a D outer pin, the inner pin must be 3 or higher.
- With a C outer pin, the inner pin must be 2 or higher.

All of this put together allows 17 combinations of inner/outer pin per chamber, and a total of 1,419,857 theoretical key differs in a five pin Classic (17^5). The number of real differs is naturally lower due to key restrictions against easy to pick patterns, master keying, and so on, but is still fairly accurate.

Master keying is provided by the use of small master pins (both inner and outer), and works like master keying in a normal pin-tumbler lock. Side (profile) pins are also available but uncommon. Master keying and side pins are discussed thoroughly in the Mul-T-Lock Interactive section.

Classic keys can be warded on both the blade and side of the key. Warding on the blade is the most common, and in the Classic warding extends the full length of the blade. The 06 keyway is the most common, with two single wards along the blade of the key (Figure 3.10). Blade warding can be used anywhere on the blade, though it is more common near the bitting area (Figure 3.11). Some Classic keys do not use blade warding at all, but instead use side warding. Most side-warded keys use a single ward down the center of the side of the key (Figure 3.12). There are other variations which use multiple wards, as well as off-center warding (Figure 3.13). Combinations of blade and side warding make for rather complex key blanks and allow for a wide range of key profiles (Figure 3.14).



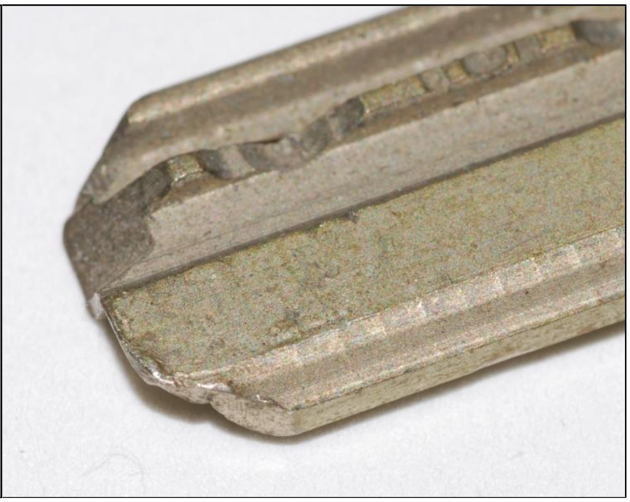
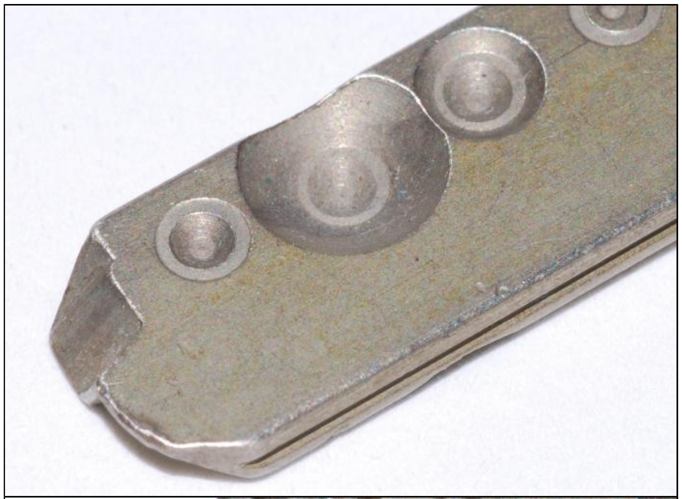
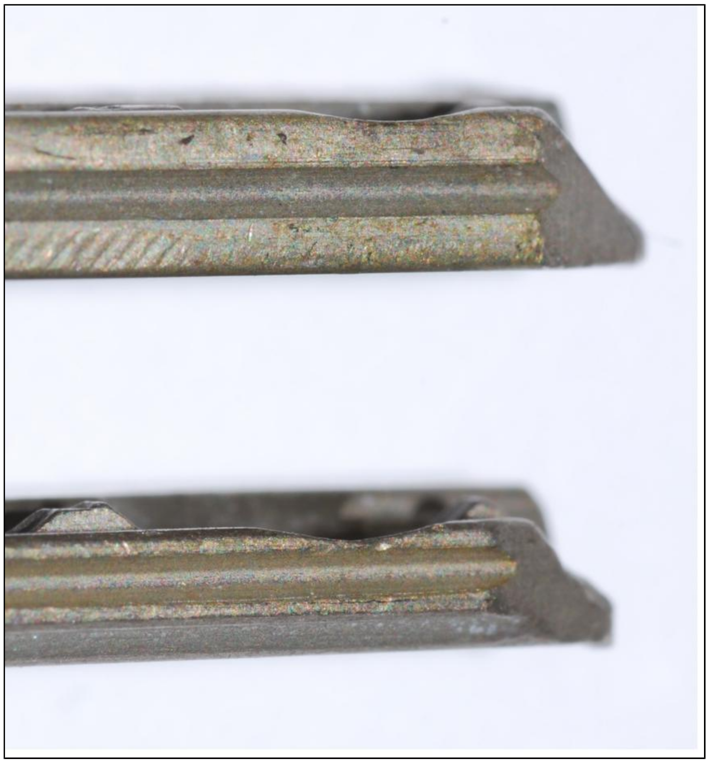


FIGURE 3.10 (Left): The 006C, by far the most common Classic key profile.
FIGURE 3.11 (Right): A Classic key with light warding on the edge of the blade.





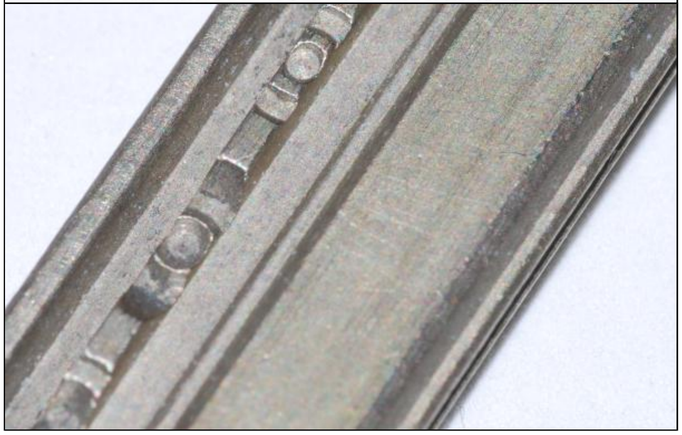


FIGURE 3.12 (Top Left): A key with no blade wards but a single side warding.
FIGURE 3.13 (Right): A comparison of side warding on two different Classic keys.
FIGURE 3.14 (Bottom Left): A key with complex blade and side warding patterns.

The Classic has three styles of key bow that identify it, two of which are unique (Figure 3.15). The most common is the black plastic square shaped bow, but key bows are available in ten different colors. The patent protection on Classic keys and key bows ended in 2007. Third party blanks are now available from a variety of manufacturers.

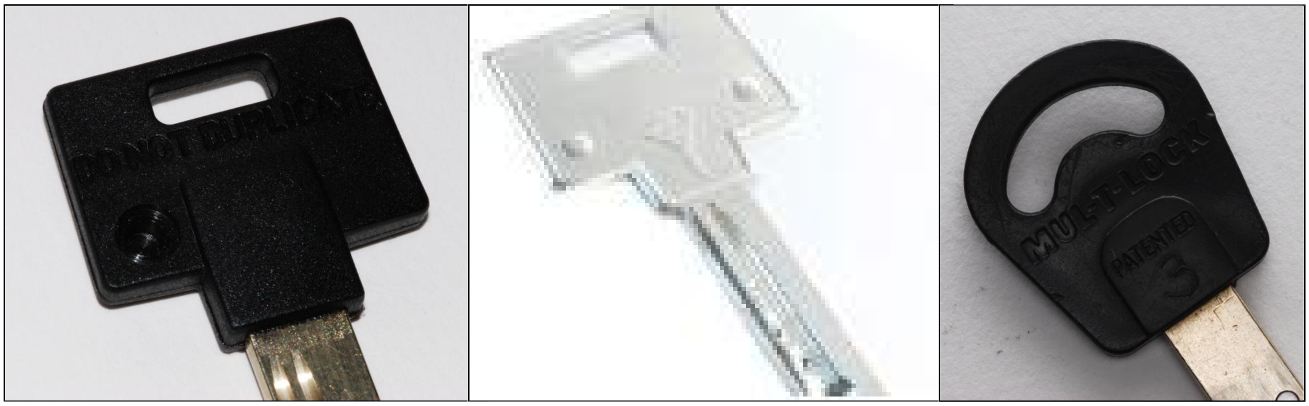


FIGURE 3.15: Classic key bow styles. The last (right) is shared with the Interactive.

Bitting Orientations

In addition to key blanks and warding, keys may be bitted on either side of the key. There are two orientations of the blank (Figure 3.16), but if we consider locks mounted "upside down" (such as European profile cylinders) there are four total. Orientations are classified by the side of the plug pins are located on and if they point up or down. Right-Up/Left-Down is the most common (Figure 3.1). Bitting orientation must be considered when choosing lockpicking tools, which we'll discuss in *Section 8, Security Analysis*.

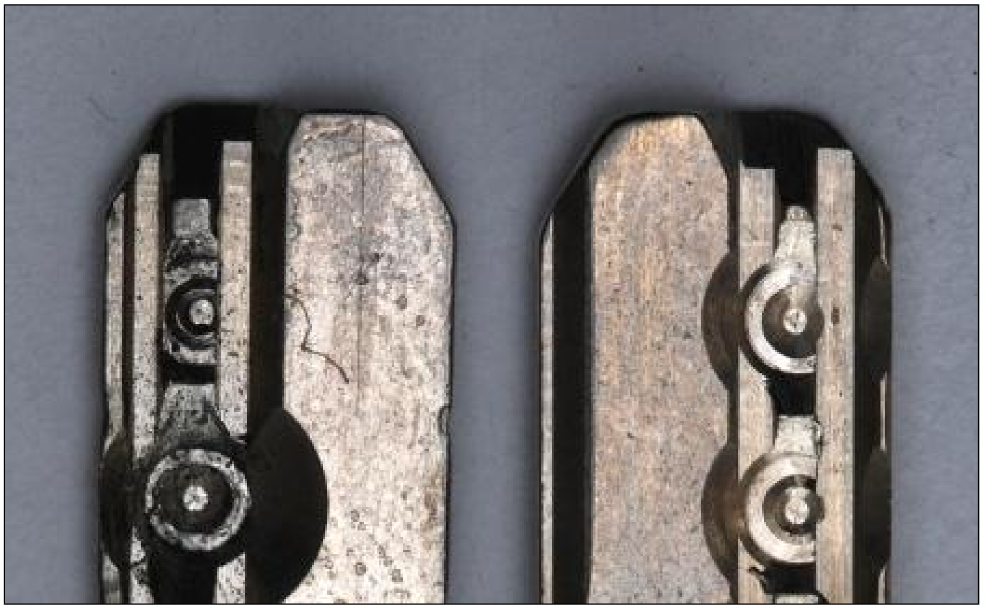


FIGURE 3.16: Left-Up/Right-Down and Right-Up/Left-Down bitting orientations.

Destructive/Forced Entry Protection

The Classic provides various additions that make it resistant to forced entry. There are two versions of anti-forced entry components. One is normal, and the other used for UL 437 certified cylinders (cylinder is stamped “UL”). The UL version provides better resistance to attack, overall. The difference is in the use of two extra steel rods in the cylinder, above the plug (Figure 3.17). More on what UL certification means in *Section 8, Security Analysis*.

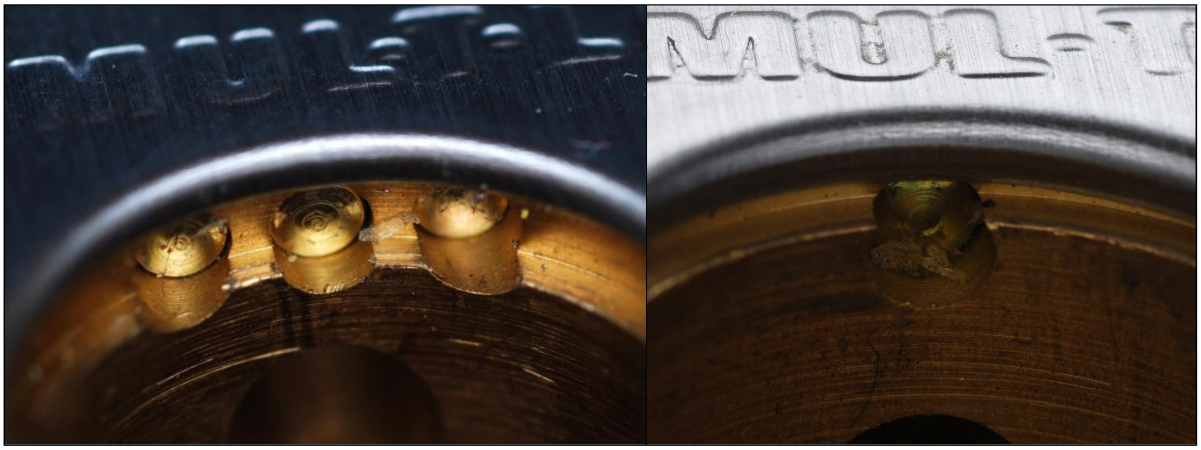
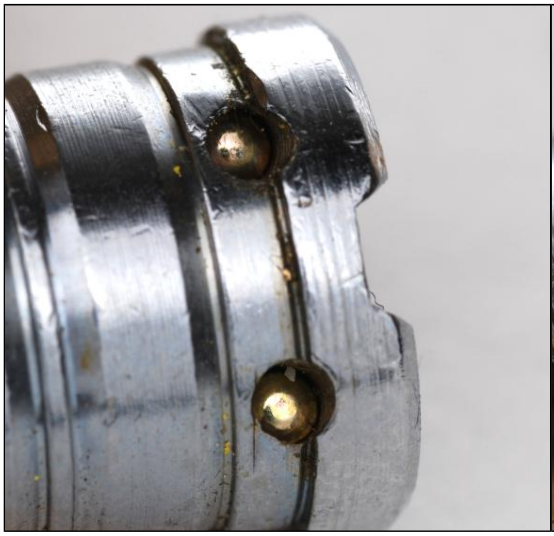


FIGURE 3.17: The UL (left) and non-UL steel rod inserts in a Classic cylinder.

The other components used, in both the UL and non-UL cylinders, are hardened steel rods above and below the keyway (Figure 3.18). Most Classics also use a ball bearing at the top of the plug, above the keyway and upper steel rod (Figure 3.19). Euro profile type cylinders may also use steel inserts in the cylinder and plug, near the second and third pin chamber.



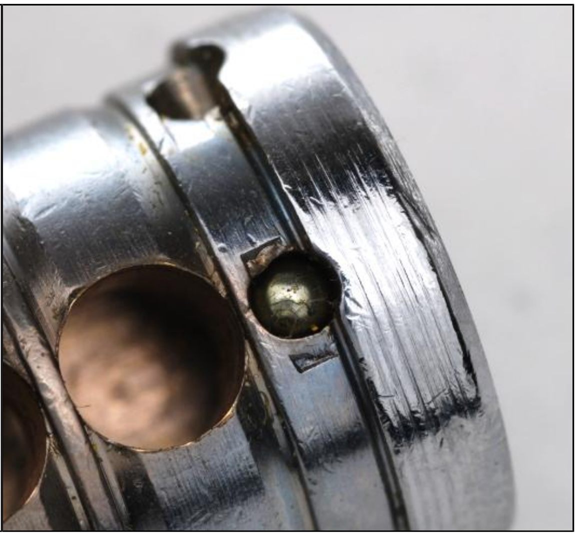


FIGURE 3.18 (Left): Hardened steel rods are inserted in the plug, above and below the keyway.
FIGURE 3.19 (Right): A ball bearing sits at the top of the plug, above the keyway and steel rods.

Classic Clones

Since the patent expired on Classic cylinders and keys, various companies now produce knock-off versions of Classic cylinders and key blanks. While they provide a similar telescoping pin system, the quality of most of these knock-offs is poor. Most do not have manufacturing tolerances as high as a legitimate Mul-T-Lock and usually do not include security pins or the anti-forced entry inserts.

Conclusion

The Classic began a rich history for Mul-T-Lock. Many of the principles of the Classic are used in other models, including modern Mul-T-Lock systems. Of course, the Classic has since been superseded by newer models, but it is still a great medium security cylinder (by modern standards) for residential use, and in my opinion is probably “good enough” for most small businesses. Now that the patent has expired most dealers have began promoting the Interactive but you can still get the Classic from many online vendors and local locksmiths.

In the next section we'll look at the second generation of Mul-T-Lock telescoping locks, the Mul-T-Lock Interactive.

4. Mul-T-Lock Interactive

Patented in 1994, the Mul-T-Lock Interactive takes the design of the Classic one step further by using a moving element in the key to interface with one of the pin stacks. It is still a four or five pin dimple lock that uses telescoping pin-tumblers but the moving element has a surprising effect on design and security. When compared with the Mul-T-Lock Classic, the Interactive provides increased security against unauthorized key duplication, key bumping, impressioning, and visual decoding.

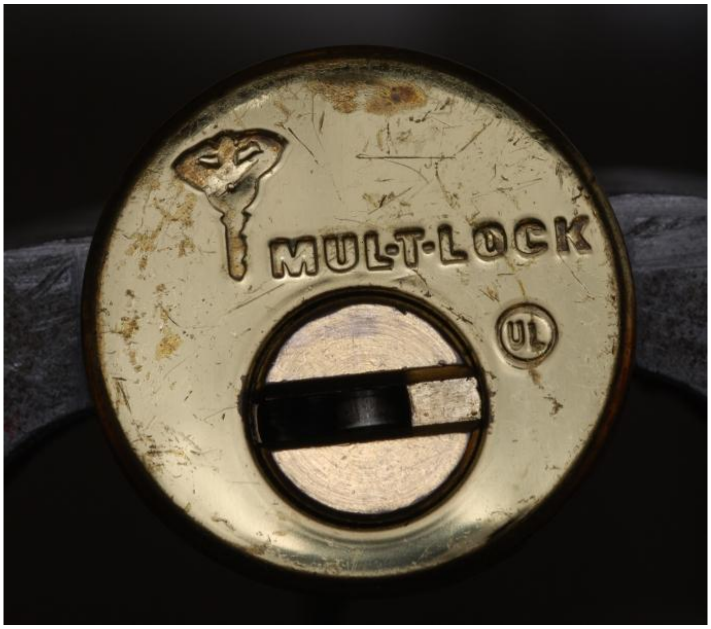


FIGURE 4.1: The Mul-T-Lock Interactive, 206 Keyway

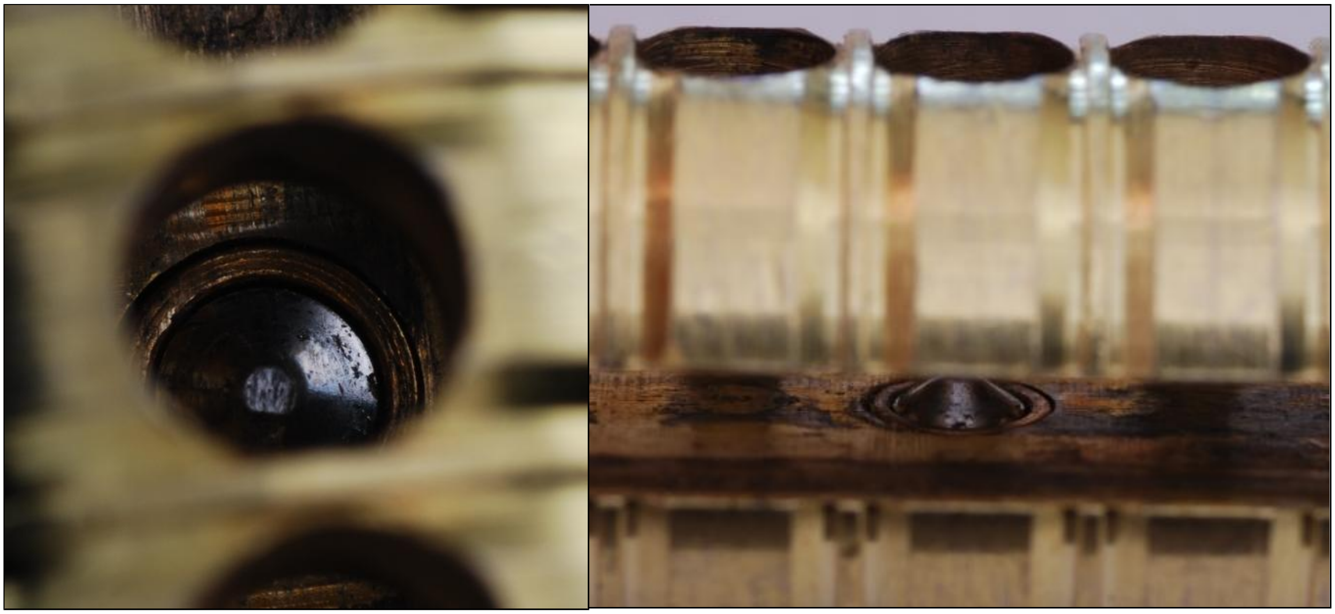


FIGURE 4.2: Top and side views of the plug's interactive chamber.

The Interactive (moving) Component

The Interactive is similar to the Classic in many ways. It uses the same pin sizes, security pin designs, and master keying scheme. Keys are tip stopped by the cam, various warding styles are used, anti-forced entry components are the same, and the key is still reversible. The main difference is that underneath one of the pin stacks is a spring-biased component that resembles a pin tip (Figure 4.2). This component interfaces with a moving element in the key (Figure 4.3), and raises the moving element to properly position the pin stack in that chamber.

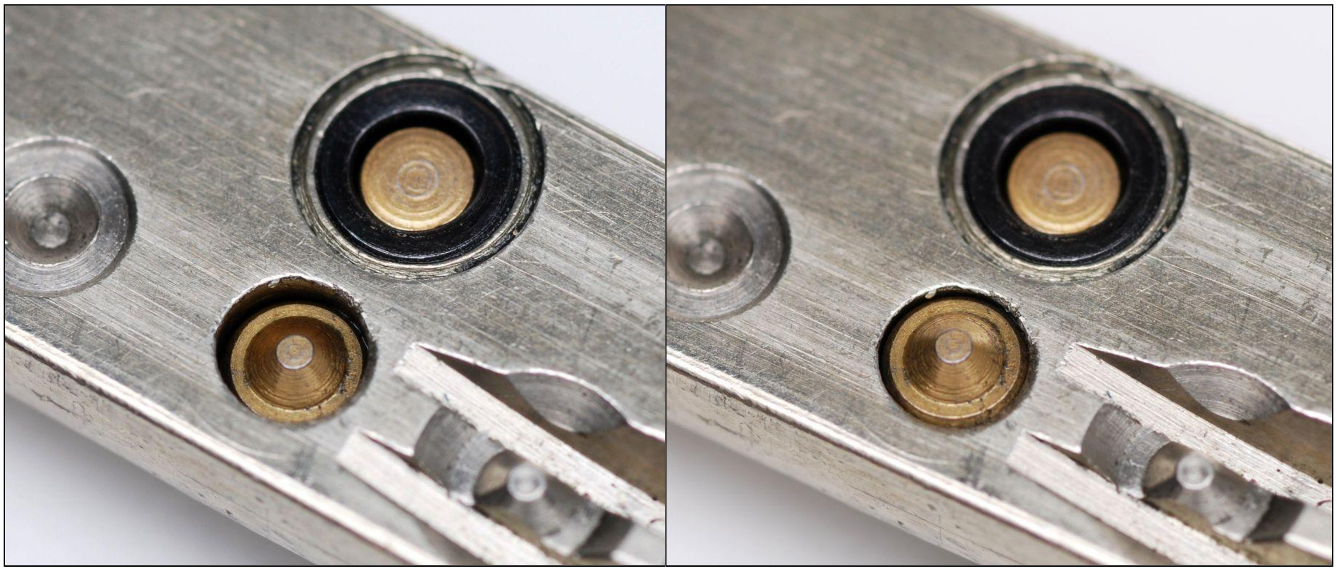


FIGURE 4.3: The key's Interactive moving element in the default (left) and raised (right) positions.

The moving element in the plug is located below the first or second pin chamber with the moving element on the key in the same position (Figure 4.4). There are two distinct moving elements in the key to accommodate for the reversible key bitting. In four pin models, the moving element is always below the first pin chamber and the key uses the second cut as the moving element – an effect of the keys being tip stopped. Having the moving element in the second chamber provides some security benefits but they are minor compared to the additional key control options of a movable position for the Interactive component. Further discussion on this will be saved until *Section 8, Security Analysis*.

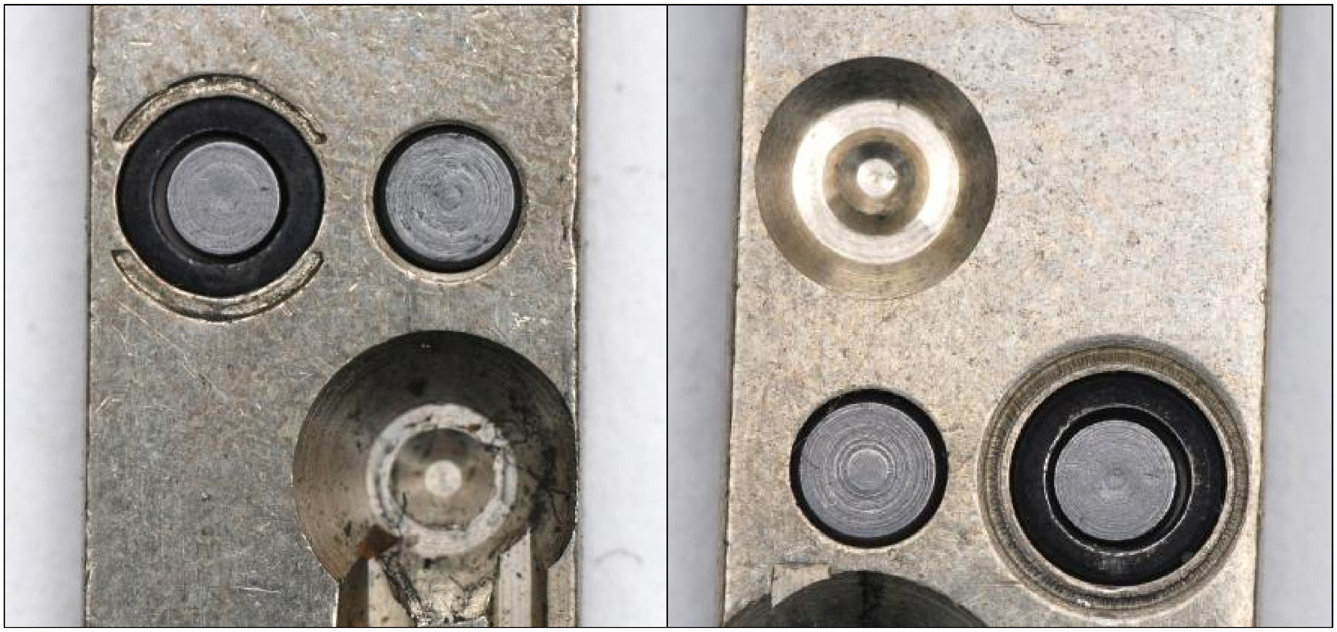


FIGURE 4.4: The Interactive moving element can be in the first or second pin position.

Simply having a moving element does not guarantee that the Interactive element will be properly positioned by the key. The Interactive uses three types of moving element (Figure 4.5). Each raises the inner/outer pins differently and must correspond to the bitting of the lock to ensure the plug will rotate. Moving elements are color coded. Each color defines how inner and outer pins are raised:

Color	Code	Type/Description	Pinning
Gold	G	Convex; raises inner pin higher	A-0
Black	B	Concave; raises outer pin higher	Z-1
Silver	S	Flat; raises both pins equally	Z-0

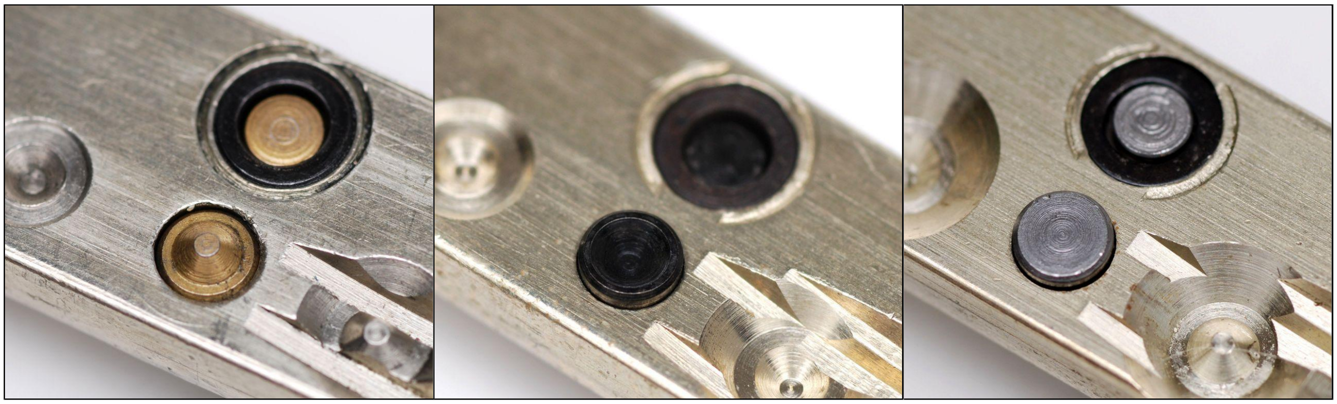


FIGURE 4.5: Left to right – Gold, Black, and Silver moving elements.

Side Pins

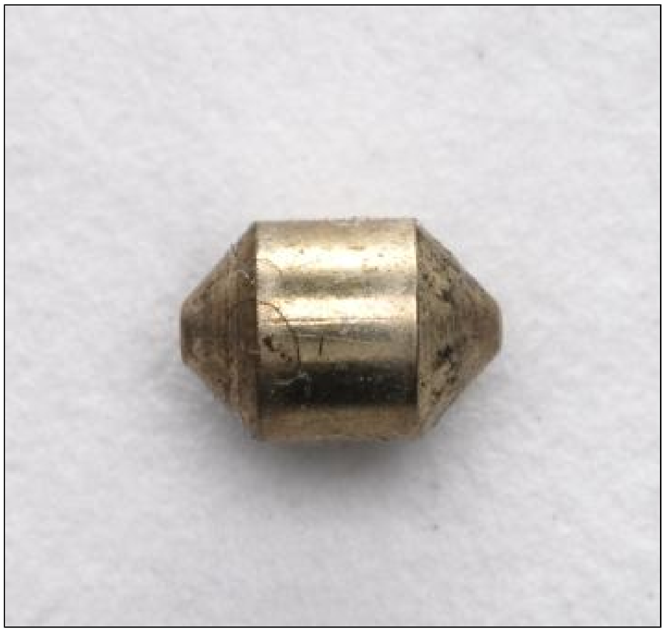


FIGURE 4.6: A Mul-T-Lock Interactive side pin.

The Classic and Interactive can also use side pins (Figure 4.6). Side pins are an optional, passive key profiling mechanism used to ensure the correct key is used. Bitting for side pins is on the side of the blade and corresponding cuts are located in the plug and cylinder (Figure 4.7).

Side pins are always located on the same side as the pins; right in a Right-Up or Right-Down lock, and left in a Left-Up or Left-Down lock. The number of side pins available is the same as the number of telescoping pin stacks; four in a four tumbler lock, and five in a five tumbler lock.

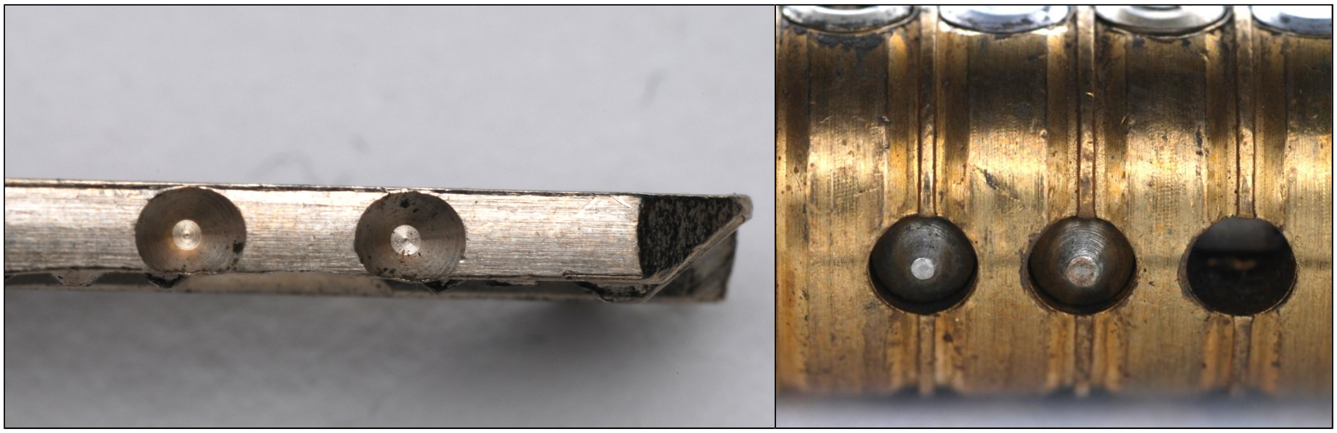


FIGURE 4.7 (Left): Side pin bitting dimples on an Interactive key.
FIGURE 4.7 (Right): Side pins in an Interactive plug. The cylinder has similar bores used to restrict plug rotation when a key with incorrect side bitting is inserted.

Keying Specifications

The moving element makes the Interactive key visually distinct. Many people mistake the moving piece for a magnet or electronic component, but they are just metal discs. (Note: *Avocet and Mottura make dimple locks that use actual magnets in the key. Both locks have keys which resemble the Interactive but perform a different function inside the lock.*)

The main advantage of the moving element is the ability to lift a pin stack higher than the top of the keyway; something a normal key cannot do. This allows additional pin sizes in the Interactive. These pins are Z and 0 (zero), for outer and inner pins, respectively. Each is a cut smaller than the Classic's smallest pins (Figure 4.8).

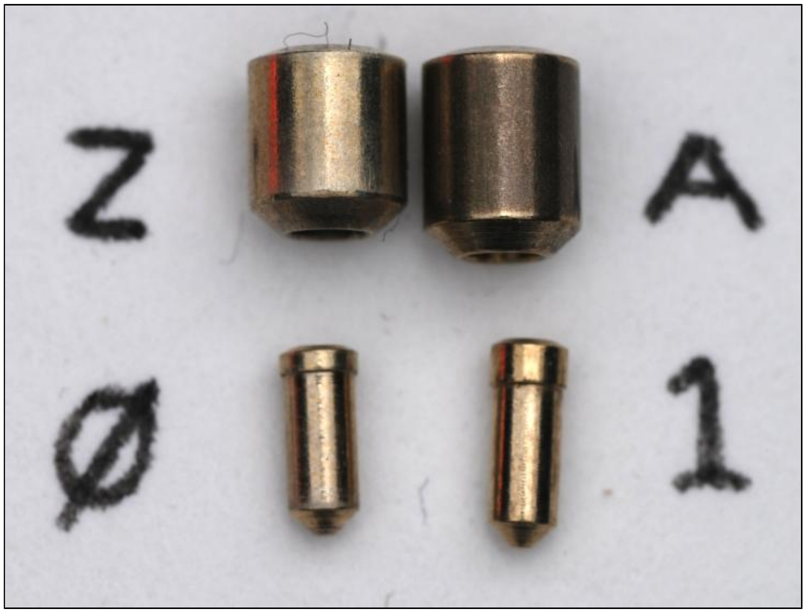
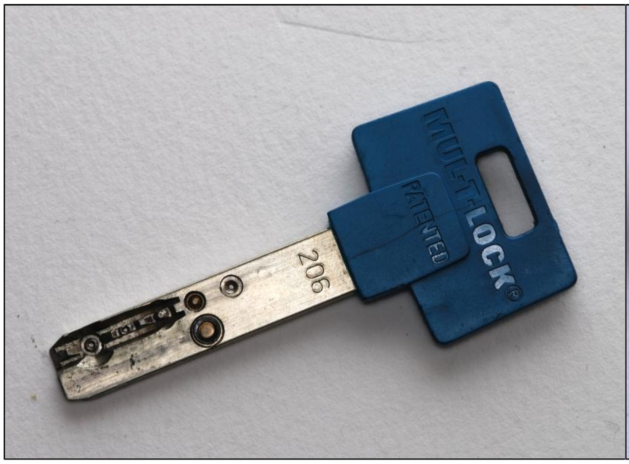


FIGURE 4.8: Interactive vs. Classic, smallest pins. Z and 0 are used in the Interactive chamber.

The moving element also prevents the ability to directly cast and impression a key, though a cast of the bitting may be used to decode the key, including the position and style of the moving element. With this information one can produce a working key on a proper Interactive blank. At the same time, machining blanks for the Interactive is harder because placement and style of the moving element must be considered.

The Interactive has downsides, though. Having only three types of pinning available for the Interactive chamber reduces our theoretical key differs to 501,126 (17^4 * 6), down about 2/3 from the Classic. The use of side pins increases this number, though that only applies if the side pins are installed. Regardless of the decrease, the number is still high enough to prevent key interchange. The difficulty in obtaining, manufacturing, or simulating Interactive keys also helps. A key with the incorrect moving element simply will not work to open the lock, regardless of the other cut depths.

Warding patterns in the Interactive are as varied as the Classic, but side warding is limited due to side pins. In spite of this, many complex warding schemes are used to provide a variety of key profiles. Like the Classic, the most common Interactive profile is the 206 (Figure 4.9), with the 2 prefix because the moving element is in the second position. While there is limited side warding, wards on the edge of the blade are common (Figure 4.10).



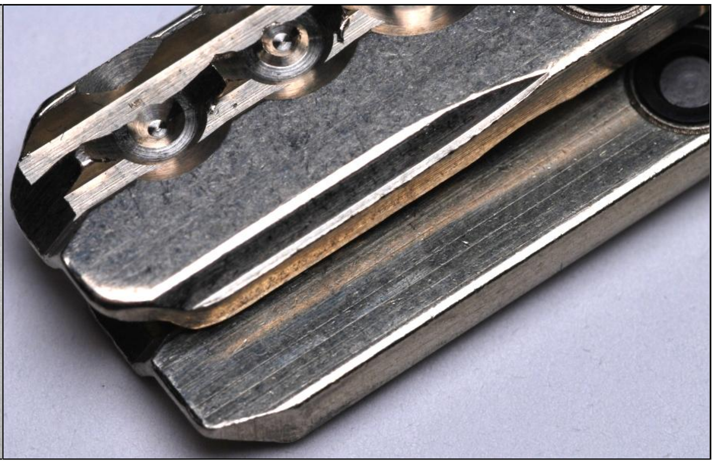


FIGURE 4.9 (Left): The Interactive 206 key profile, with the G (Gold) moving element.
FIGURE 4.10 (Right): Interactive keys with and without warding on the edge of the blade.

One important distinction is that Interactive keys can never have warding extend past the moving element. The moving element is restricted to the first two chambers because you couldn't heavily ward a key with it in the fourth or fifth position. Even if you did, it is likely an attacker could just file down the tip of a key to bypass the wards. This also means Interactive cylinders will never have visible warding. As a result, the keyway profile of an Interactive lock cannot be casually observed without looking deep into the keyway (which may be problematic because of the pins), trying common key profiles until one works, or observing a working key. It also means that any lock *with* visible warding cannot be an Interactive.

The Interactive uses three styles of key bow, two of which are unique (Figure 4.11). The rounded plastic design is shared with the Classic, but examination of the key to identify the moving element can clear up any confusion. The patent for Interactive keys expires in 2014.

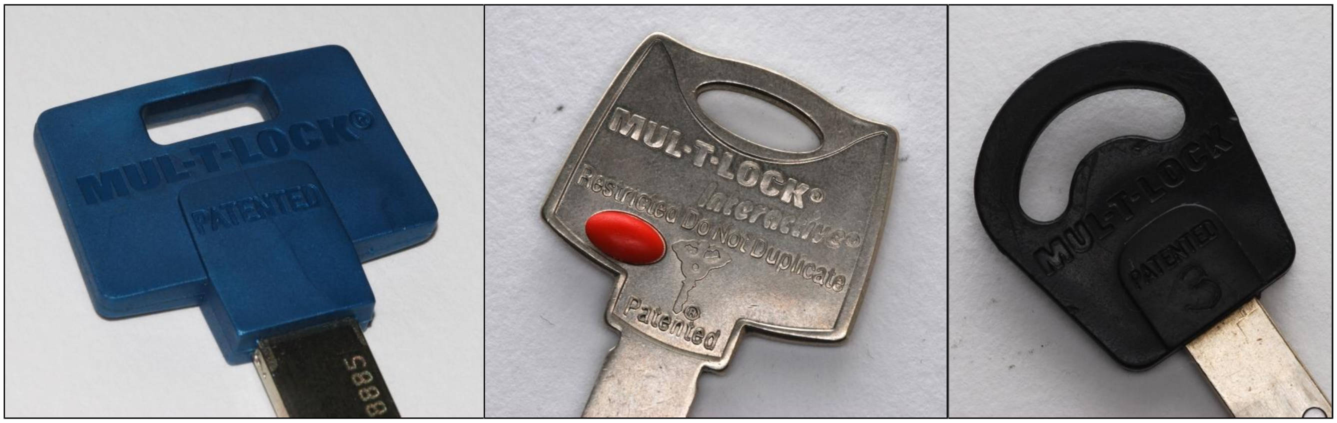


FIGURE 4.11: Mul-T-Lock Interactive key bows. The first two are unique to the Interactive.

Master Keying

The Classic and Interactive models provide for complex master keying systems through the use of three types of traditional master pins (Figure 4.12).

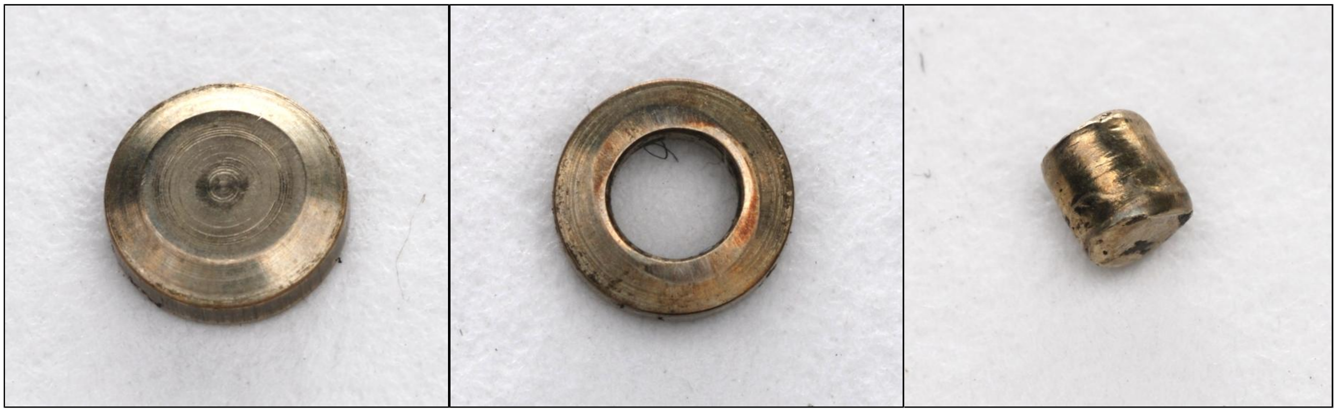


FIGURE 4.12: Three styles of master pins used in Classic and Interactive models.

The solid master (4.12, left) provides master keying for both inner and outer pins. The external master (4.12, center) and the internal master (4.12, right) provide master keying for individual pin stacks. The external and internal masters are often combined to avoid MACS problems between inner and outer pins. There are 4 sizes available for inner master pins and 3 sizes available for external master pins. The pinning for inner master pins is designated 1 to 4, with 4 being the largest pin. External master pins are 1 to 3, with 3 being the largest. The gauge shown lists them in millimeters instead of by code (Figure 4.13).

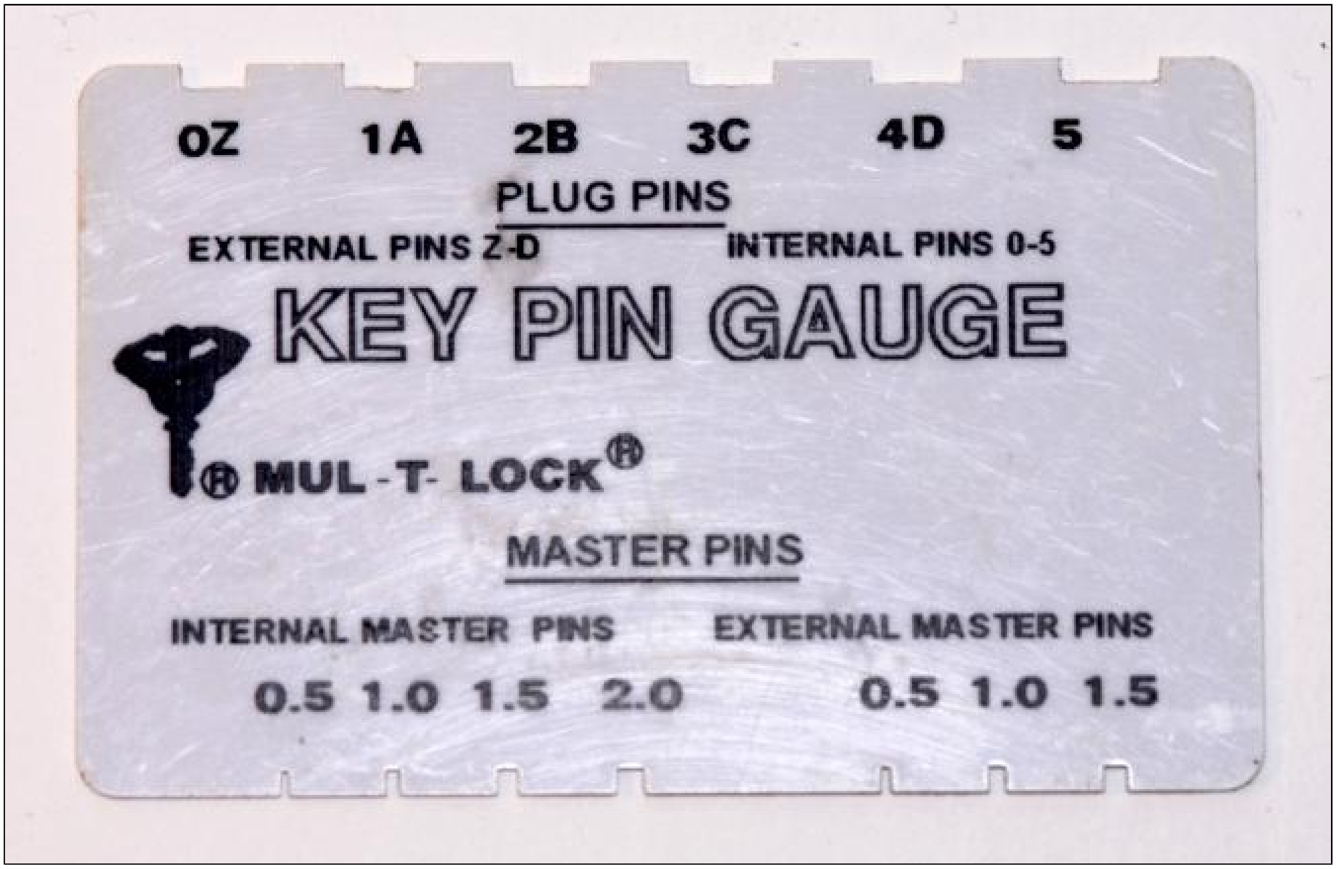


FIGURE 4.13: A Mul-T-Lock Classic/Interactive key gauge with 0/Z and master pins included.

Of course, when using master pins we must consider the pinning rules when master keying locks. This isn't too hard if we consider all pins to be numbered. For example, with any inner pin we add its value to the master pin, and if that number is higher than 5 it can't be used. The same goes for outer pins, but with a maximum of 4 (D).

Using the inner or outer master pins individually is trickier, because we need to consider the MACS between inner and outer pin stacks. Again, all we need to do is run the numbers to make sure we're within our limits. I'll leave figuring out the math up to you :)

In addition to the three traditional master pins, three types of solid key pins can be used. These each have their own pin codes based on what shape they are (Figure 4.14). These shapes are similar to the floating pin styles; X- is a convex key cut, XX is an even key cut, and X+ is a concave key cut. Each of the solid pins can be combined with solid master pins (4.12, left) for additional master keying requirements.

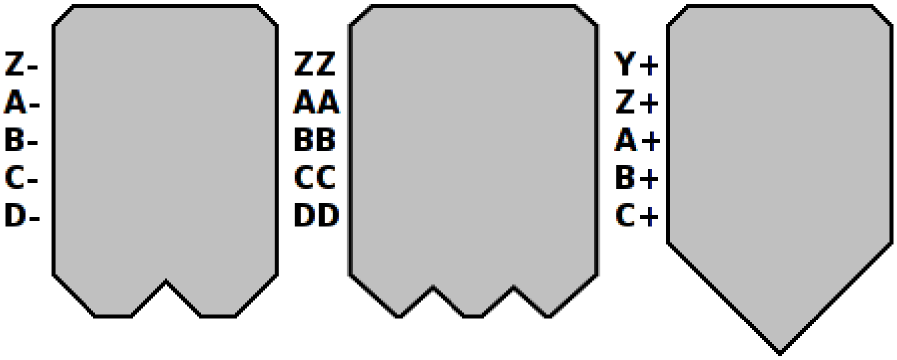


FIGURE 4.14: Solid key pin shapes and codes used in master keying.

Of course, using the solid master pins drastically reduces the number of real key differs for a given lock. A normal telescoping chamber will have 17 combinations of pins, but the solid pin chambers will only have 5. Again, more can be added with solid master pins, but this is at the expense of pick resistance and key interchange. Why use solid key pins? They were implemented, to my knowledge, as a standard part of master keying to defend against the Michaud attack. The Michaud attack is discussed in-depth in *Section 8, Security Analysis*.

Conclusion

The Mul-T-Lock Interactive is in many ways an improvement over the Classic, offering a variety of additional and improved security features. Of those, the inability to directly cast a key is important, as well as the troubles associated with obtaining or creating the correct key blanks. The difficulty in visually decoding the keyway profile of an Interactive is an interesting side-effect of the design of the Interactive component, one that makes many techniques, especially bumping, more difficult.

In the next two sections we'll discuss variations on the Interactive design, the CLIQ and 3-in-1.

5. Mul-T-Lock CLIQ

Note: All the photos in this section (unless otherwise noted) are taken by and used with permission of Eric Schmiedl (http://www.ericschmiedl.com).

Introduced in 2004, the Mul-T-Lock Interactive CLIQ is a combination of the Interactive cylinder with an electronic authentication system known as CLIQ.

Developed by ASSA-Abloy for their other product lines, the CLIQ was made available to Mul-T-Lock after they joined the ASSA-Abloy family in 2000. The CLIQ system is used in several other ASSA-Abloy locks, such as the ASSA Twin and Abloy Protec.

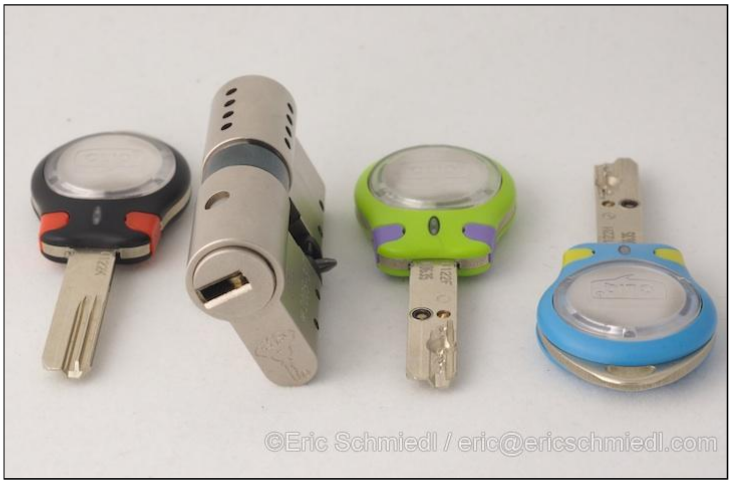


FIGURE 5.1: The Mul-T-Lock CLIQ, Euro profile.

The mechanical portions of the key and lock are mostly the same as the Interactive so we'll skip discussion of them. The main difference between Interactive and CLIQ locks are the CLIQ components on the bow of the key and inside the plug and cylinder of the lock itself.

The electronic components on the key bow make these keys stand out when compared with other Mul-T-Lock keys (Figure 5.1). Key bows are oval and come in a variety of different colors. When disassembled, we see that the bow is actually hollow with electronic components placed inside of it (Figure 5.2).

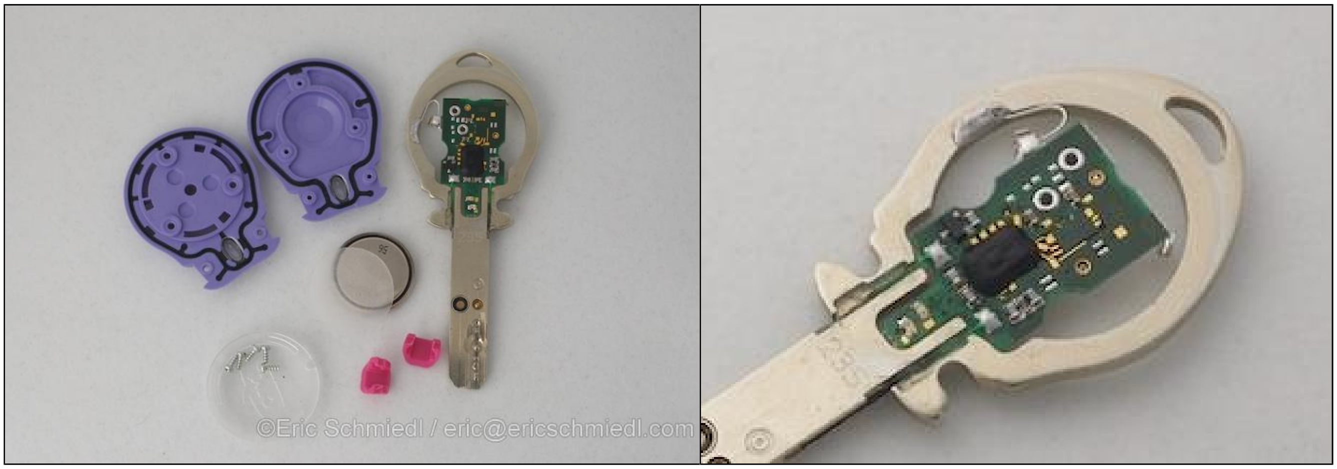


FIGURE 5.2: Disassembled and close-up view of the Interactive CLIQ key's electronics.

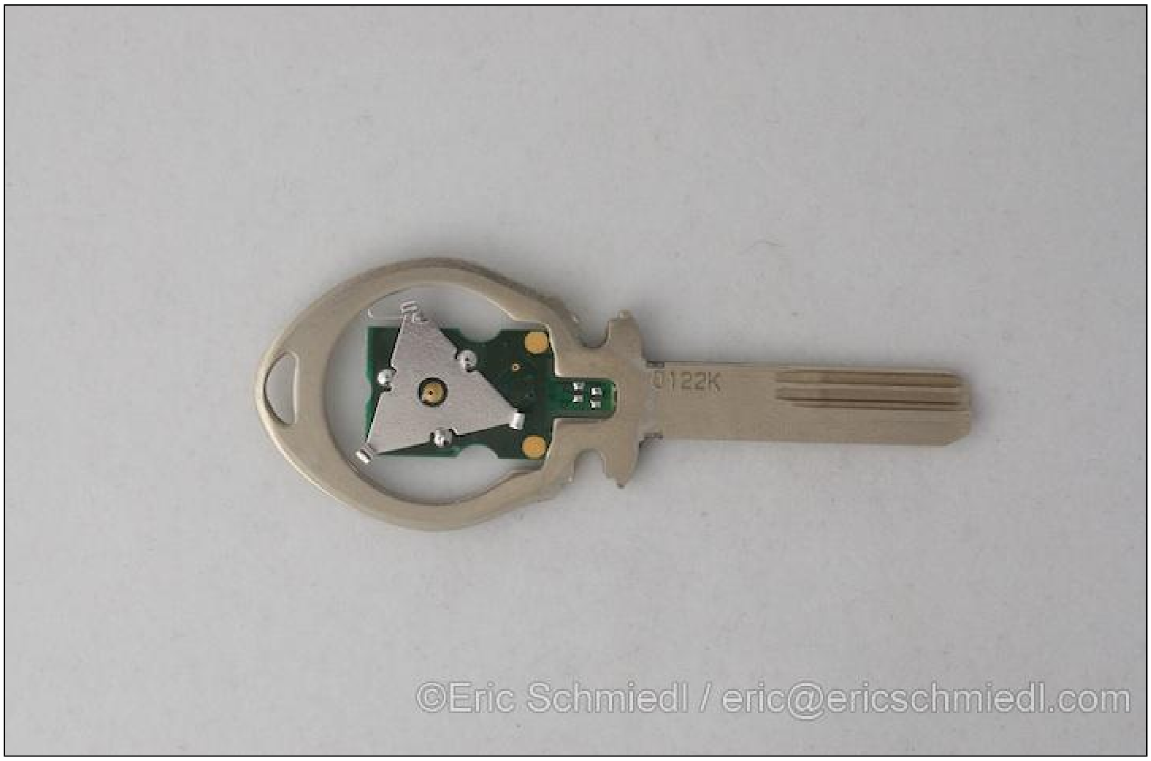
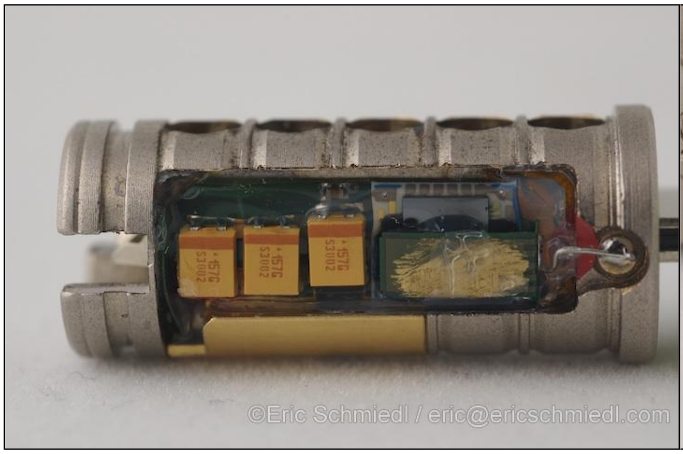


FIGURE 5.3: Control key with CLIQ electronics exposed. Note the lack of bitting cuts.

Control keys (“C-keys”) look similar to user keys but they are used to reprogram the lock's internal CLIQ electronics and read the audit log. Control keys cannot actually open the lock because they do not contain any bitting cuts or Interactive element (Figure 5.3).

Inside the lock, a large portion of the plug is replaced with electronic components to power the CLIQ (Figure 5.4). At the bottom of the cylinder and plug, a sidebar-like system is used by the CLIQ to restrict rotation of the plug until authentication has taken place (Figure 5.5).



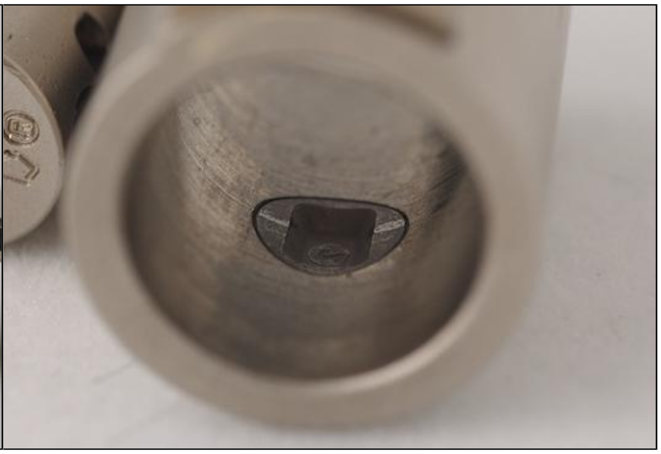


FIGURE 5.4 (Left): The Mul-T-Lock CLIQ plug with the electronics shown.
FIGURE 5.5 (Right): The Mul-T-Lock CLIQ cylinder with sidebar recess shown.

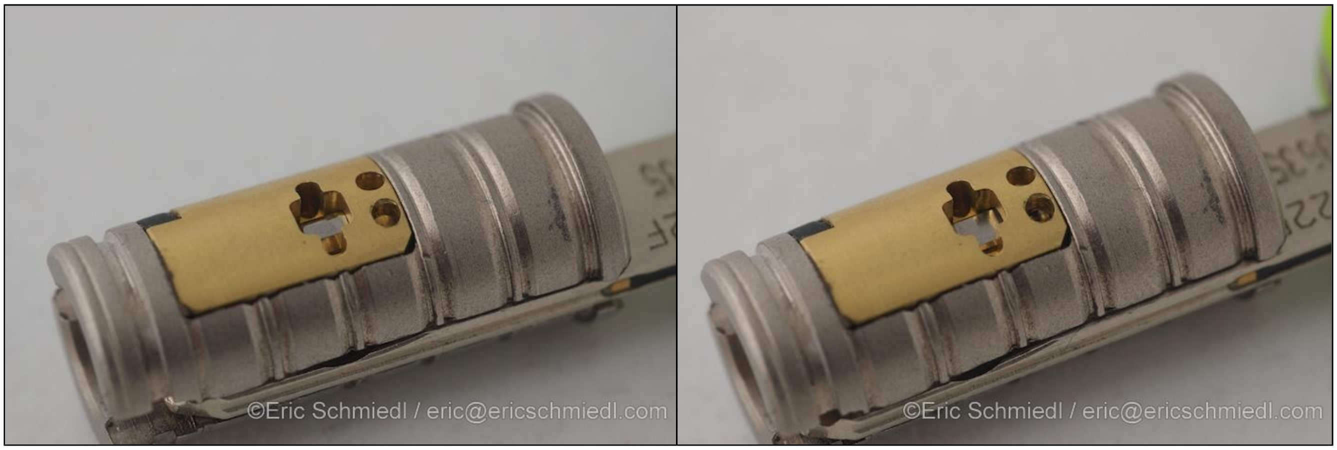

©Eric Schmiedl / eric@ericschmiedl.com
©Eric Schmiedl / eric@ericschmiedl.com

FIGURE 5.6: The CLIQ plug restricting (left) and retracting (right) the sidebar controls. (Note: The actual sidebar component is *not* shown.)

The CLIQ sidebar is unconventional; it's shape is similar to a large side pin, similar to the side pin used in the Schlage Everest lock. Once authentication is successful the electronics rotate a blocking piece to allow the sidebar to drop into the plug (Figure 5.6). Assuming the telescoping pins are also properly aligned, the plug can now rotate and unlock the lock. The CLIQ components inside of the lock are not battery powered, but instead are powered by inserting the key. If authentication is successful the LED on the key bow will blink green. If not, it will blink red. In either case, the CLIQ stores audit logs of authentication successes and failures (the last 1,000 attempts). Audit logs can be read from the lock using the control key.

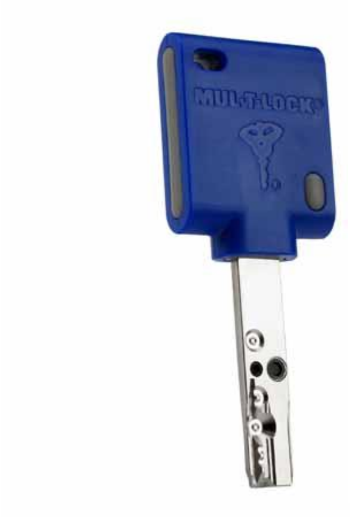
Electronic Communication

When a contact on the side of the key (visible in Figure 5.6) contacts the inside of the lock, the key sends a small pulse to power on the lock. Mul-T-Lock refers to this as a “wake-up signal.” Once awake, the plug generates a random 64 bit number and broadcasts a challenge. The key answers by encrypting its own number and sending it to the plug. The plug decrypts the number and compares to its own. If the numbers match, the sidebar is released and the plug can rotate. Unfortunately, I don't have more detail on this process. Please contact me if you can help!

Communication between the CLIQ key and lock takes place with 3DES encryption and claims to offer 2^{64} possible authentication token combinations. Management of CLIQ authentication tokens is provided by Mul-T-Lock through a variety of software packages and the reprogramming keys. Of course, master keying with the CLIQ is considerably simplified compared to traditional, mechanical master keying because of the relative ease with which keys can be added and removed from the electronic system. At the same time, the addition of traditional master keying with a CLIQ system's electronic method may be preferred for sensitive installations as an added precaution. A more thorough discussion of CLIQ security and possible attacks is located in *Section 8, Security Analysis*.

SynerKey / SynerCLIQ

A similar system is the SynerKey, which is a traditional Interactive key with a RFID transponder in the key bow (Figure 5.7). These are not CLIQ locks, but they do have their own special key bow. An upgraded version of this is known as the SynerCLIQ, which is a CLIQ system with transponder included in the CLIQ bow. The SynerCLIQ can be identified because the key bow has a distinct logo when compared to normal CLIQ keys (Figure 5.8).



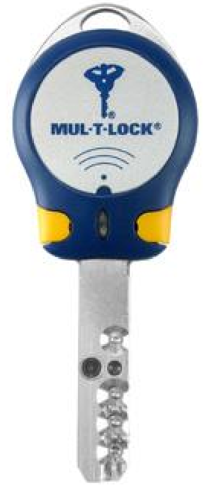


FIGURE 5.7 (Left): The SynerKey (non-CLIQ) Interactive key
FIGURE 5.8 (Right): The SynerCLIQ Interactive key

Conclusion

The CLIQ is one of Mul-T-Lock's most complex models. It provides the same basic anti-forced entry components as the other models, but the electronic element makes covert and surreptitious attacks harder. The actual security of the CLIQ is currently a hot topic. Research by Jord Knaap, Marc Tobias, Tobias Bluzmanis, and Barry Wels identified various electronic and mechanical design flaws. More on this in *Section 8; Security Analysis*.

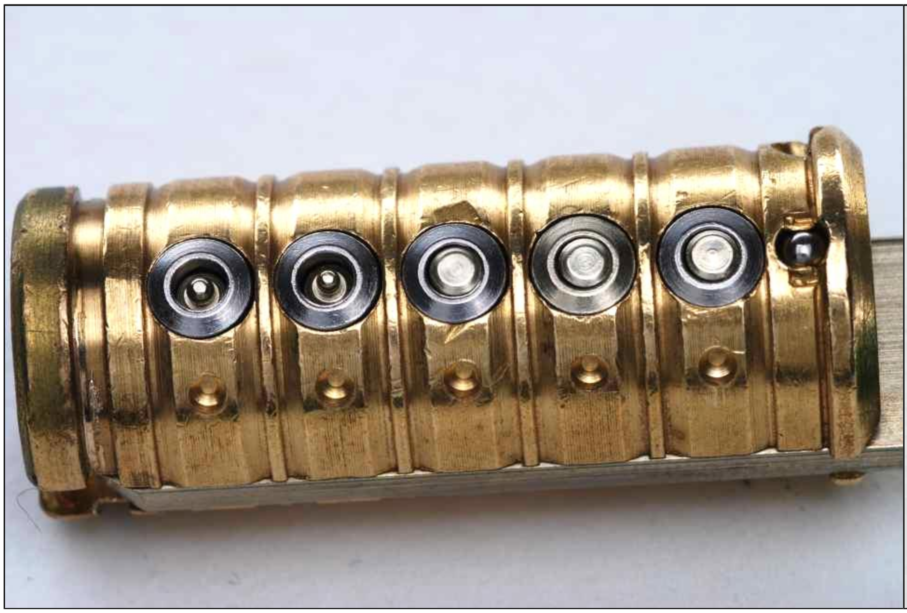
While the CLIQ uses the Interactive components and similar key, it is currently unclear whether or not the 2014 patent expiration date for the Interactive will affect the ability to obtain CLIQ blanks, or at least those without an electronic component. I would guess this isn't the case, but I'm not sure. Please contact me if you can answer this; contact information is available in the introduction to this paper.

At the time of writing this the Mul-T-Lock Interactive CLIQ is considerably more expensive than almost all other Mul-T-Lock models, with cylinders alone retailing at $700-1000 USD. While it provides a high level of security, it is cost prohibitive for all but the most sensitive installations. The SynerKey may be an effective alternative for small to medium sized installations.

6. Mul-T-Lock 3-in-1

The 3-in-1 is a user-rekeyable form of the Classic and Interactive systems. It allows the user to progressively re-key the lock up to two times given a set of pre-supplied keys. This section will focus on the Interactive 3-in-1. There are Classic versions of the 3-in-1, but their internals are the same. Unlike the CLIQ, which uses the same Interactive components, the 3-in-1's re-keying function changes the internals slightly. In a nutshell, the 3-in-1 is a construction keying system that takes advantage of the telescoping tumblers to provide re-keying.

In a traditional construction keying system a ball bearing is placed in one of the pin stacks. When user keys operate the lock the ball bearing remains below the shear line, acting like a master pin. When the construction key is used the ball bearing is raised above the shear line and the cylinder is turned. When the plug is rotated, the ball bearing falls into a bore on the side of the plug and is removed from the pin stack. At this point, the previous (non-construction) keys do not work. The 3-in-1 functions on the same principle, except it uses a break-away component on inner pin stacks instead of a free-floating ball bearing.



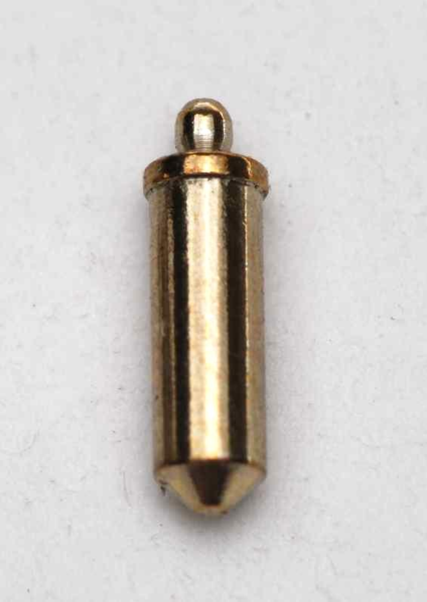


FIGURE 6.1 (left): 3-in-1 plug, with modified inner pins and construction keying bores.
FIGURE 6.2 (right): 3-in-1 inner pin with breakaway ball on the top.

When disassembling the 3-in-1 there are two oddities (Figure 6.1). First, construction keying bores are located on the side of each pin chamber on the plug. The bores are considerably smaller than the outer pin stacks. Second, some of the inner driver pins have a modified design. When removed from the pin stacks, the inner pins used for construction keying each have a small ball at the top (Figure 6.2). All other pins in the lock are standard.

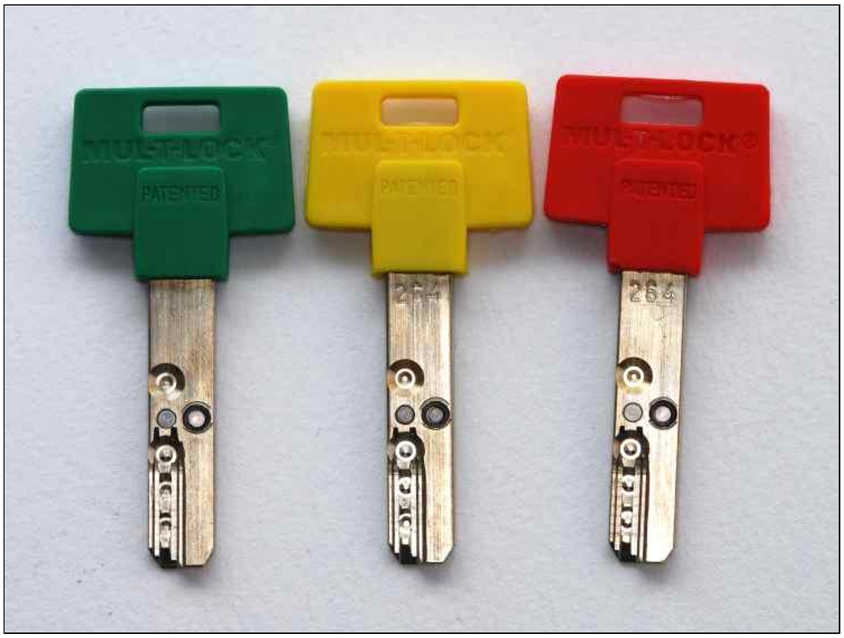
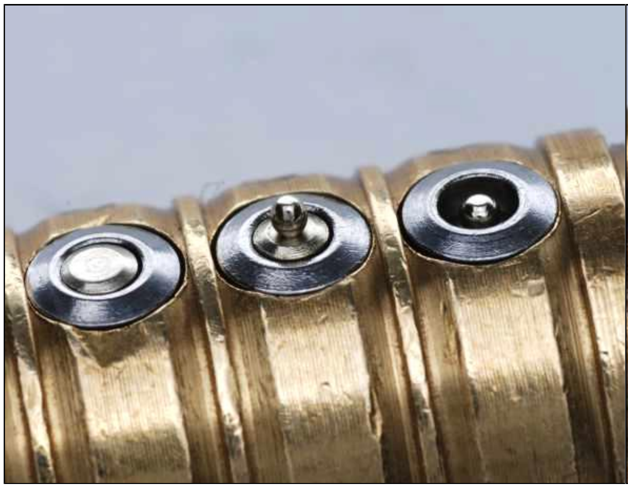


FIGURE 6.3: The 3-in-1 system uses a color progression to signify access levels.

The 3-in-1 comes with three different color keys. Each key color represents a level of access in the 3-in-1 system. From lowest to highest, they are green, yellow, and red (Figure 6.3). When the lock is brand new, only the green keys work. The green keys raise all construction pins high enough that the top of the construction ball aligns with the shear line (as in Figure 6.1). When it is time for the keys to change, the yellow key is inserted. This raises one of the construction balls above the shear line (Figure 6.4). The yellow key is then forcibly rotated and the ball snaps off, creating a new shear line. Rotating the plug allows the ball to fall into the bore on the plug, removing it completely from the pin stack (Figure 6.5). At this point only the yellow key can operate the lock.



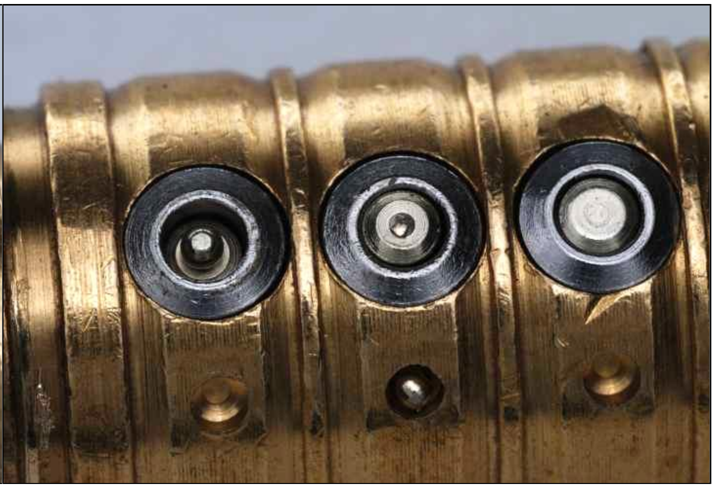


FIGURE 6.4 (Left): The yellow key raises the inner pin's ball above the shear line.
FIGURE 6.5 (Right): Use of the key breaks the ball and drops it into the plug bore.

After the yellow key is used we can again re-key the lock with the red key. The same logic applies; the red key is inserted, it will raise the other ball above the shear line. Note that if we wanted to we could go straight to red, as it will raise both balls above the shear line (Figure 6.6). In either case, we snap off the remaining balls with rotation of the key and they are deposited into the plug bores (Figure 6.7). At this point, only the red key will operate the lock.

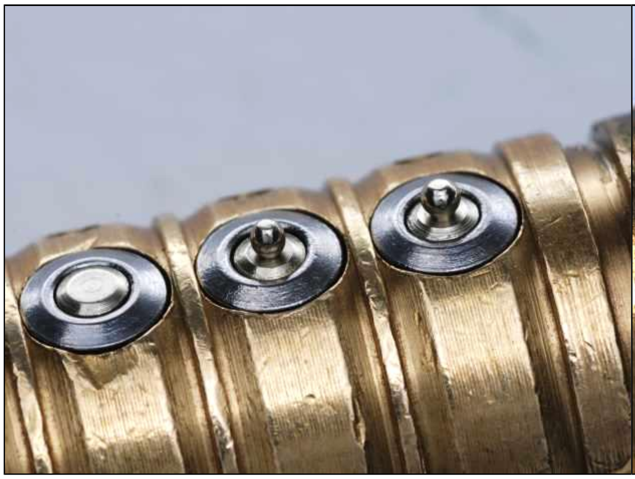
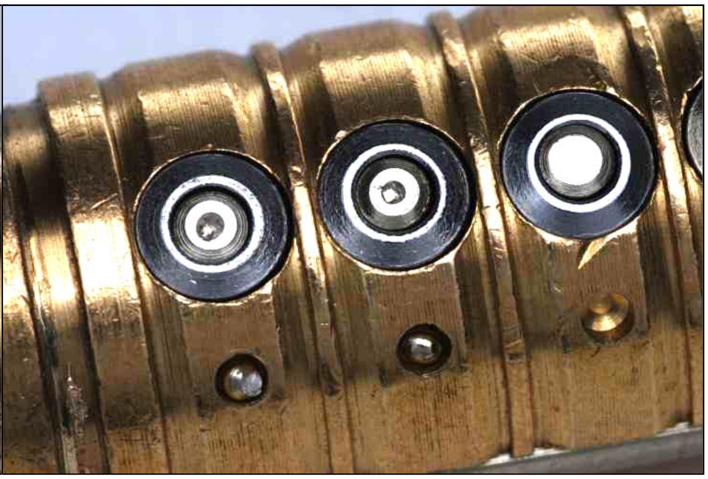



FIGURE 6.6 (Left): The red key raises all balls above the shear line.
FIGURE 6.7 (Right): Use of the key breaks the balls and drops it into the plug bore.

3-in-1 keys are easily identified because factory original keys follow a green-yellow-red bow progression and only use the square plastic key bow design. Being normal Interactive keys, 3-in-1 keys may be reused in traditional Interactive cylinders and vice versa. Again, while Classic keys may also use the same bow and colors a quick examination of the key can determine if it has the Interactive component.

In the Classic 3-in-1, the Black square plastic bow is commonly used with colored bow inserts to signify keying level. The same may be done for other key styles and bows if keyed by a locksmith.

Conclusion

The 3-in-1 is a fairly simple construction keying implementation using Mul-T-Lock's telescoping pin system. It is a variation of the traditional Classic and Interactive designs but for the most part it functions in exactly the same way. The 3-in-1 can technically be made into a five level system, but few real-world applications require that much re-keying in a short period of time!

The next section will discuss Mul-T-Lock's newest systems, the MT5 and MT5+.

7. Mul-T-Lock MT5/MT5+

The newest Mul-T-Lock design is the MT5, dubbed so because it is the fifth generation of Mul-T-Lock's telescoping pin system. Introduced in 2007, the MT5 contains the standard telescoping pins and a new moving element called the Alpha spring. The MT5+ version also uses a slider-based sidebar system.

This section will focus on the MT5+ but the MT5 model is essentially the same thing without the sidebar. In my experience, when people refer to the MT5 they are usually talking about the MT5+, anyways!

The MT5+ is a major change to the previous Mul-T-Lock designs. It is a high-security cylinder that offers additional key control and resistance to compromise when compared to previous Mul-T-Lock models.

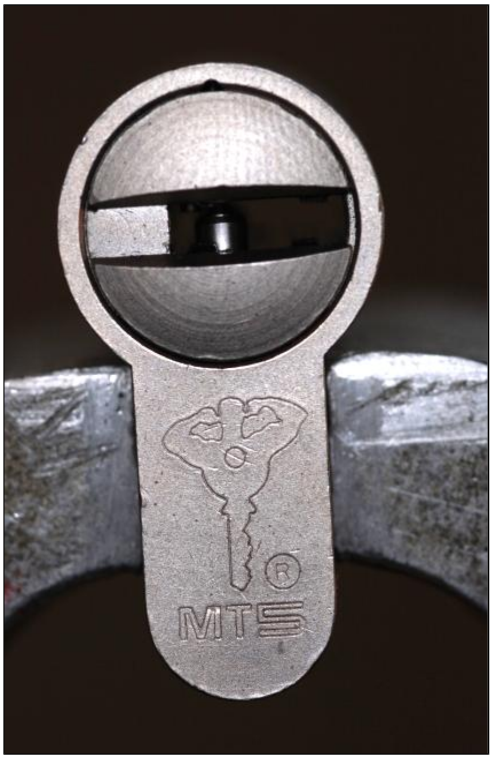


FIGURE 7.1: The MT5+, 05 keyway

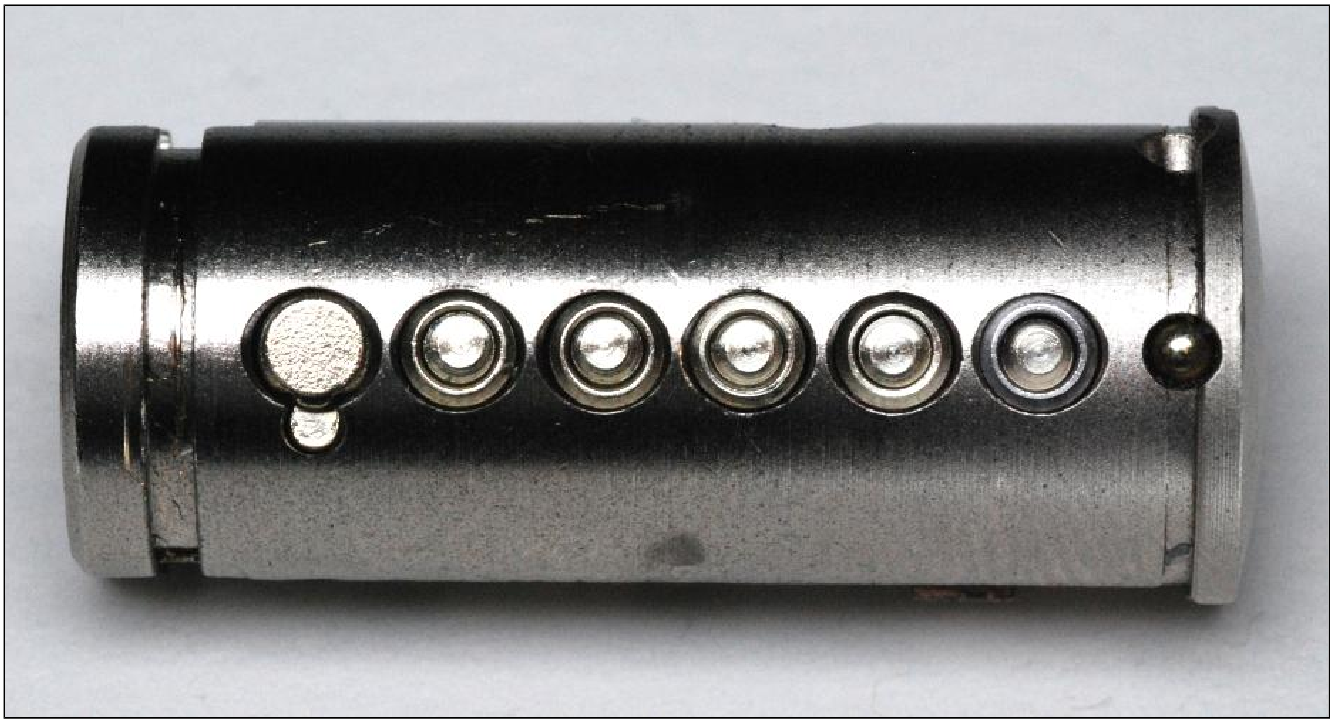
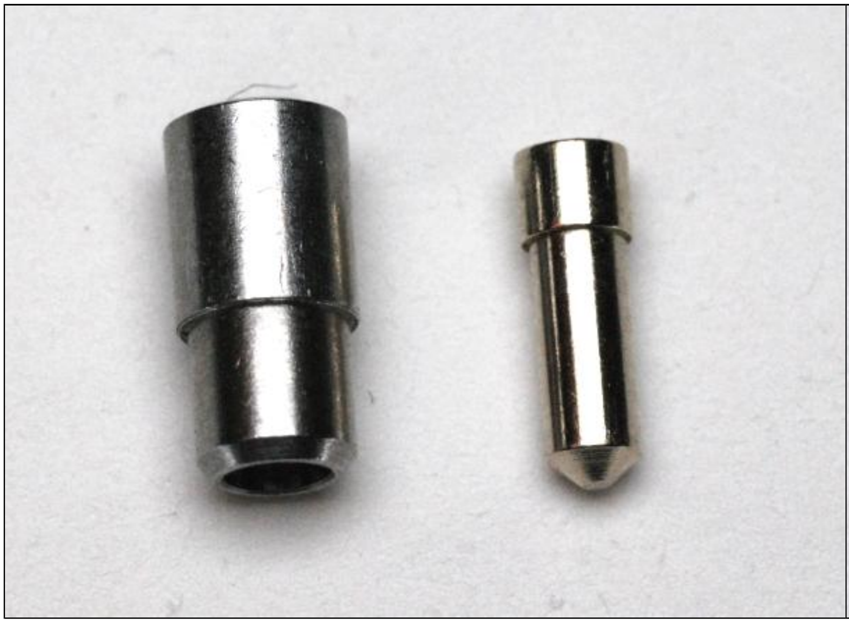


FIGURE 7.2: Top view of the MT5/MT5+ plug, showing five telescoping pin pairs, Alpha chamber (far left), and anti-forced entry ball bearing (right).

The primary locking components in the MT5 are a set of five telescoping pin-tumblers (Figure 7.2). Unlike the Classic and Interactive, which share pins, the MT5 and MT5+ use a new set of key pins (Figure 7.3). Driver pins look the same as they did in the older models and serrated are again the security pins of choice. The sixth pin chamber is used for the Alpha spring, the new moving element. Pins in this chamber are not telescoping and are quite unique (Figure 7.4).



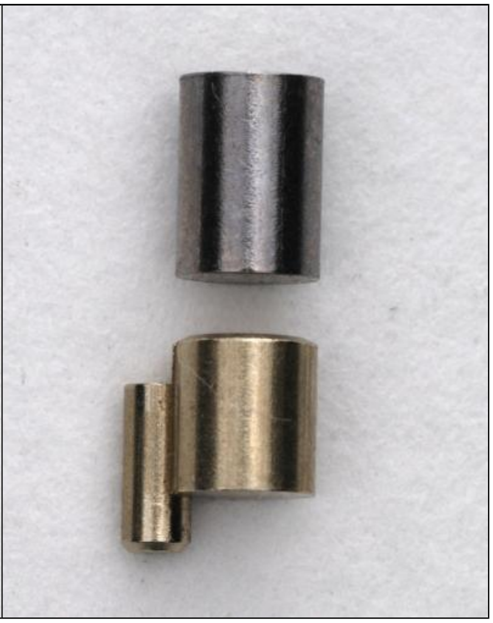
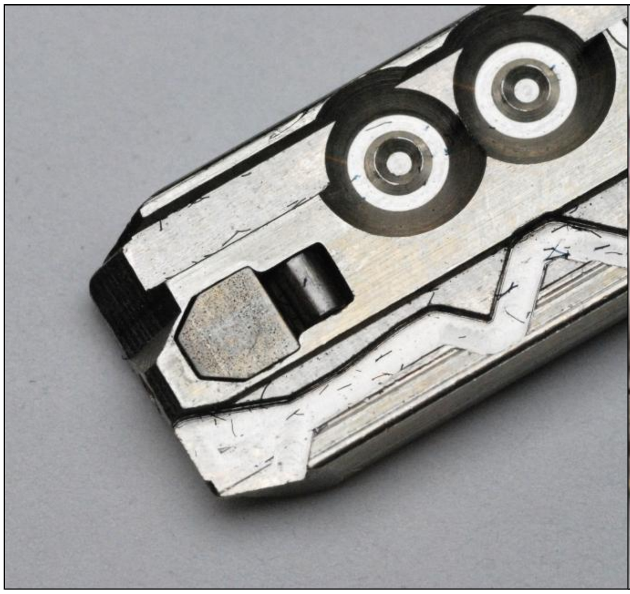


Figure 7.3 (Left): MT5/MT5+ key pins, slightly different design than older models.
Figure 7.4 (Right): Driver and key pins of the Alpha spring chamber (pin six).

Alpha Spring

The Alpha spring sits near the tip of the key (Figure 7.5) and interacts with the sixth pin-tumbler pair. When the key is inserted the plug walls pinch the Alpha spring *into* the key. Once fully inserted, the plug walls push the Alpha spring up to raise the pin in the Alpha chamber (Figure 7.6). The pin it raises is very interesting. First, it is not telescoping but instead a traditional pin-tumbler pair. The chamber used to hold the Alpha pin stack only exposes the protrusion on the key pin (Figure 7.7). Looking at the key, we notice the Alpha spring sits in the center of the key, away from the bitting area. This makes the Alpha spring symmetrical with respect to key orientation and leaves more space for warding on the key blade (as compared to the Interactive).

Like the Interactive, the Alpha spring prevents the ability to directly cast a working key. Instead, a cast of the bitting cuts may be used to decode the key and produce a working key. All MT5 and MT5+ models currently use the same Alpha spring; there's no variation in the pin size or position of the Alpha chamber. This is strange given the Interactive's variety but it seems to be the case in the United States and abroad.



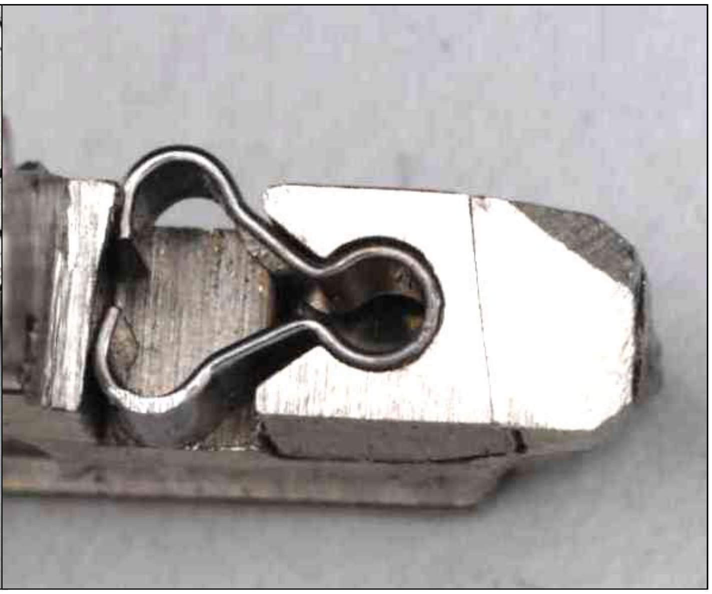


FIGURE 7.5 (Left): The Alpha spring component at the center of the tip of the key.
FIGURE 7.6 (Right): The Alpha spring component (cutaway key) is raised by the plug walls.

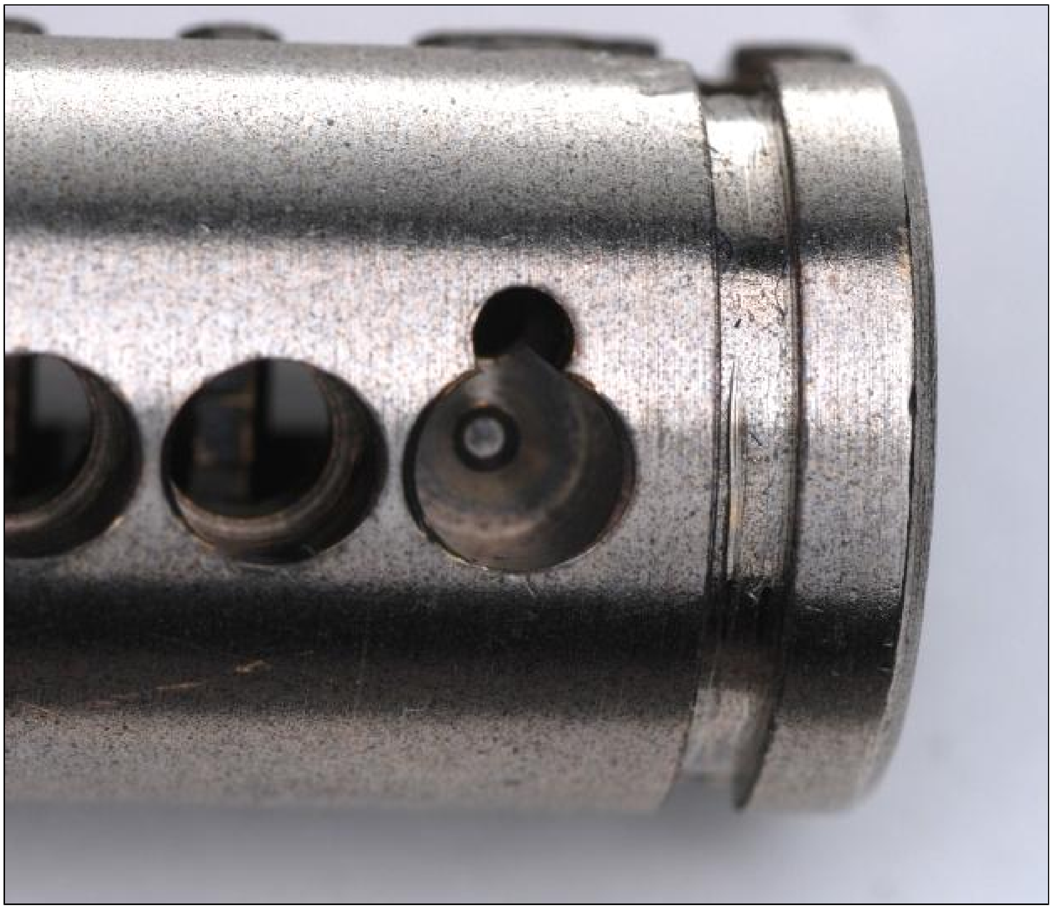
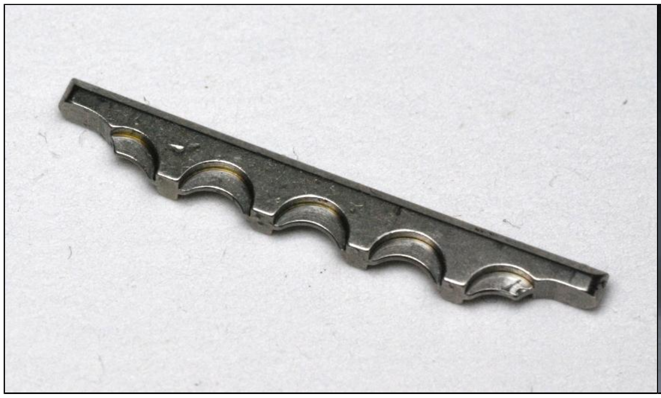


FIGURE 7.7: The Alpha chamber is not drilled like a traditional pin chamber.
Instead, it only exposes the protrusion on the key pin.



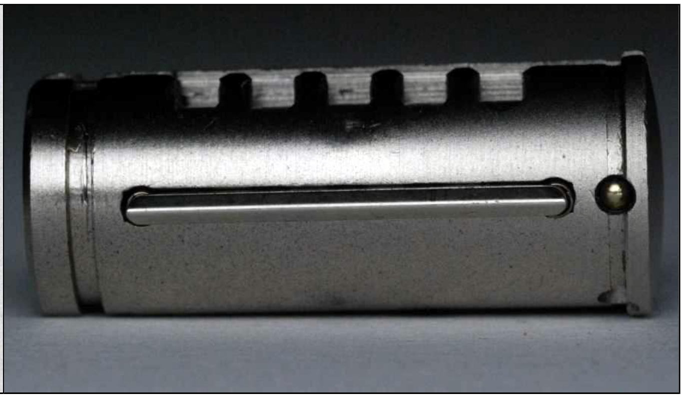


FIGURE 7.8 (Left): The MT5+ sidebar. Actuated by five free-floating sliders.
FIGURE 7.9 (Right): The MT5+ sidebar is located on the *bottom* of the plug.

MT5+ Sidebar

MT5+ models have one major improvement over the MT5 — the use of a sidebar (Figure 7.8). The sidebar is made of nickel-silver and is positioned in the 6 o'clock position, the bottom of the plug in the American configuration (Figure 7.9). Five free-floating sliders (also called 'finger pins') interact with the sidebar through the use of small gates. Pick resistance is provided by false gates surrounding the true gate (Figure 7.10).

Locksmiths who can create MT5+ keys do so by using blanks which have no sidebar bitting defined. A key card associated with every lock is used to create keys with a MT5+ key machine. Attacks on duplicated/counterfeit MT5+ keys are discussed more thoroughly in *Section 8, Security Analysis*.

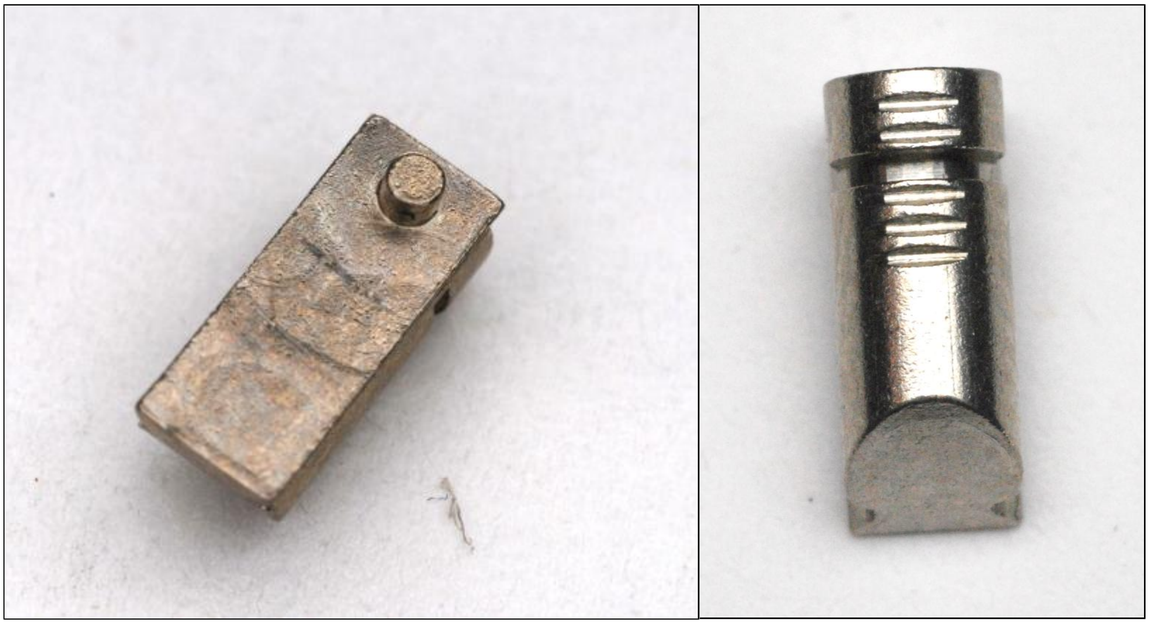


FIGURE 7.10: MT5+ slider. The top (left) interfaces with a track on the key, and the bottom (right) interfaces with the sidebar. Note the anti-picking false gates.

When viewed in the plug, sliders are positioned horizontally, located underneath and in-between telescoping pin-tumbler stacks (Figure 7.11). When all sliders are properly aligned the sidebar can fall into their true notches and plug rotation is no longer restricted (Figure 7.12).

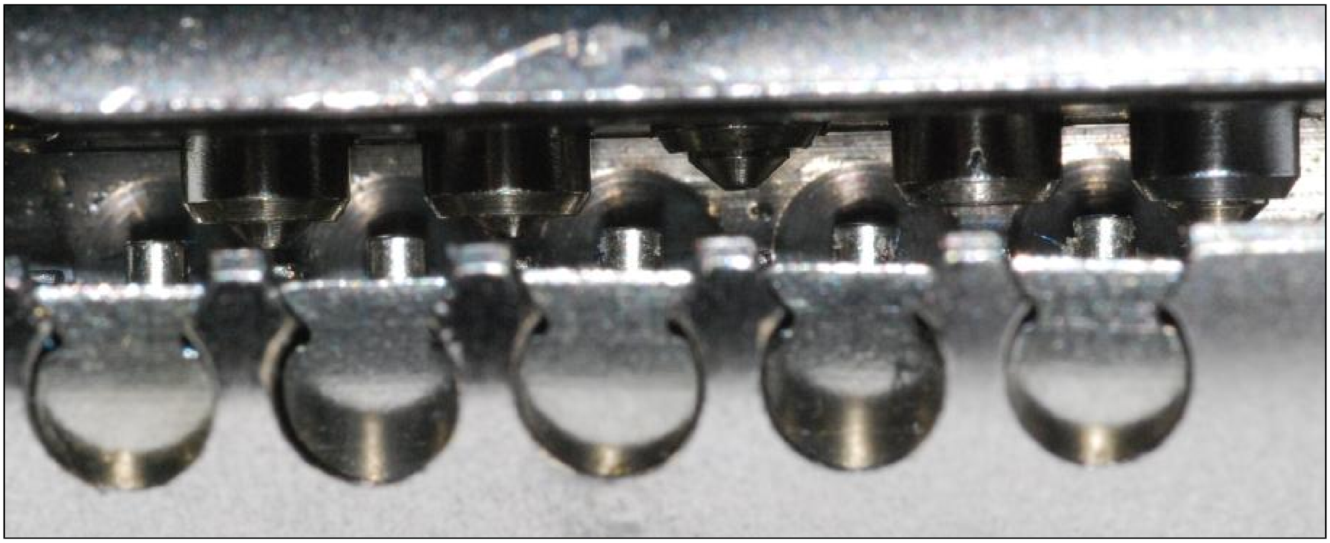


FIGURE 7.11: Inside view of the plug, showing arrangement of telescoping pins and sliders.

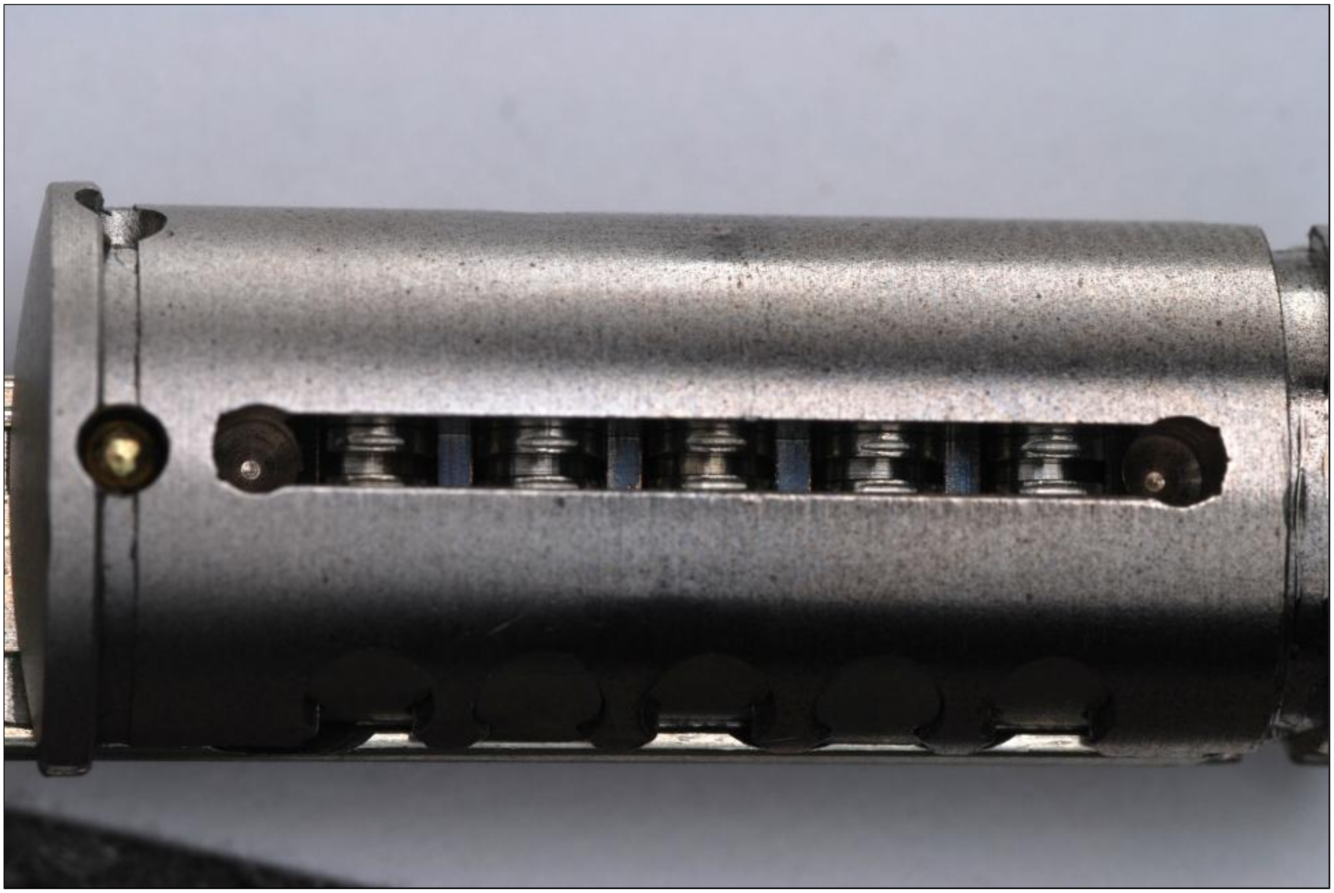


FIGURE 7.12: MT5+ sliders properly aligned, the sidebar can now be retracted and plug rotated.

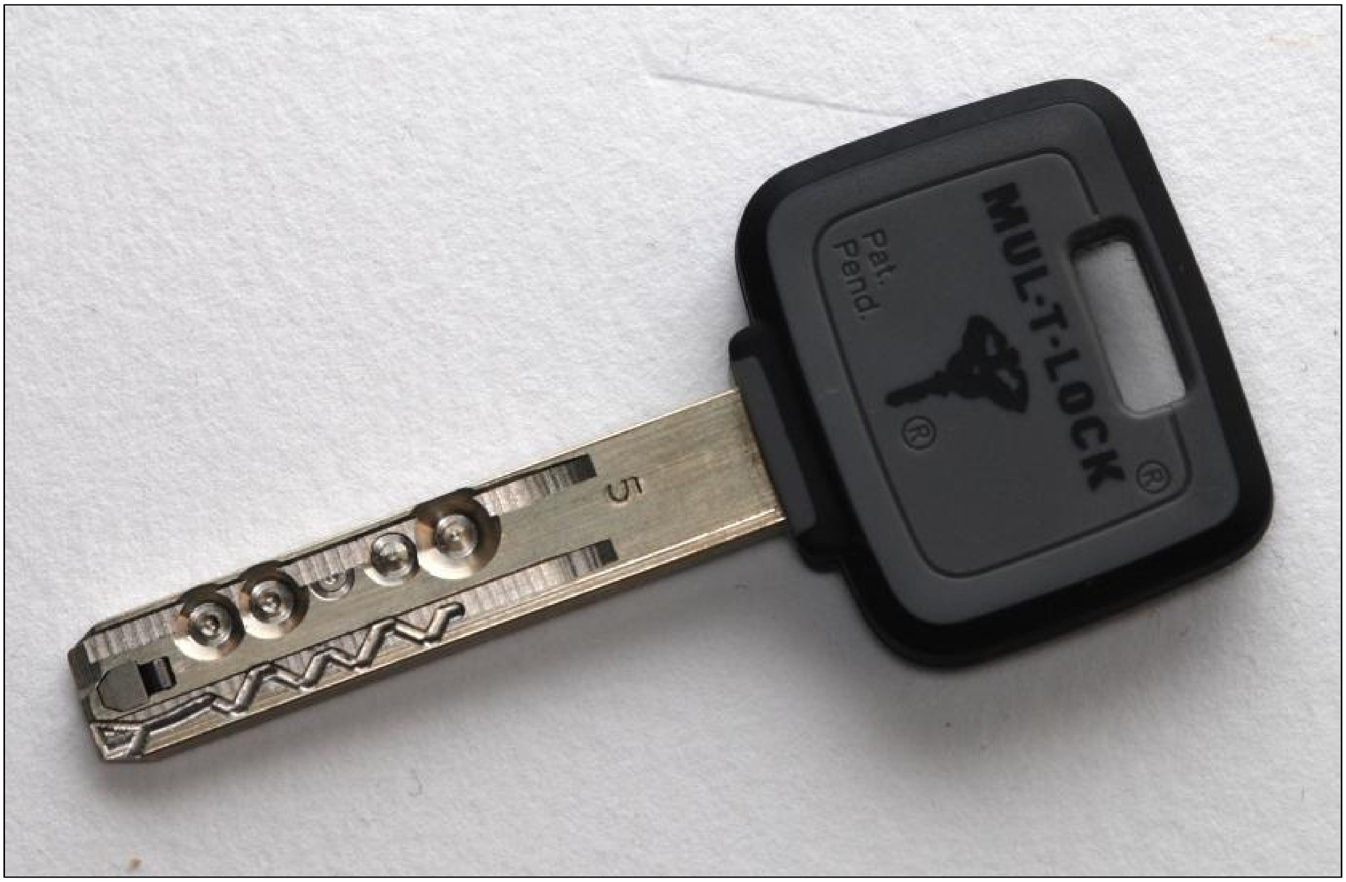


FIGURE 7.13: The MT5+ key with telescoping bitting, Alpha spring, and sidebar track.

Keying Specifications

The normal MT5 key works much like a traditional Mul-T-Lock telescoping key — almost the same as the Interactive. Five telescoping pins must be properly positioned and the Alpha spring raises the pins in the sixth chamber. The MT5+ key is unique due to the use of a sidebar (Figure 7.13).

The most interesting feature of the MT5+ key is that it uses both the top and bottom of the blade. One side is used for the telescoping pins and the other for the sidebar pins. Though both versions use the traditional telescoping pin cuts, the MT5+ uses a milled track for the sidebar pins, commonly referred to as a “laser track” in the automotive locksmithing industry. This is similar in appearance to other sidebar slider bittings, such as those in the Scorpion CX-5 and the EVVA 3KS.

Like the earlier models, the MT5/MT5+ has 4 depths for outer pins and 5 depths for inner pins (Figure 7.14). Unlike the Interactive, the alpha spring does not add any extra pin depths to the lock. In the MT5+ model, there are 5 positions for slider pins. Keying codes for the MT5+ are extended to include finger pin bitting (EP-IP-FP; “exterior” pins-”interior” pins-”finger” pins).

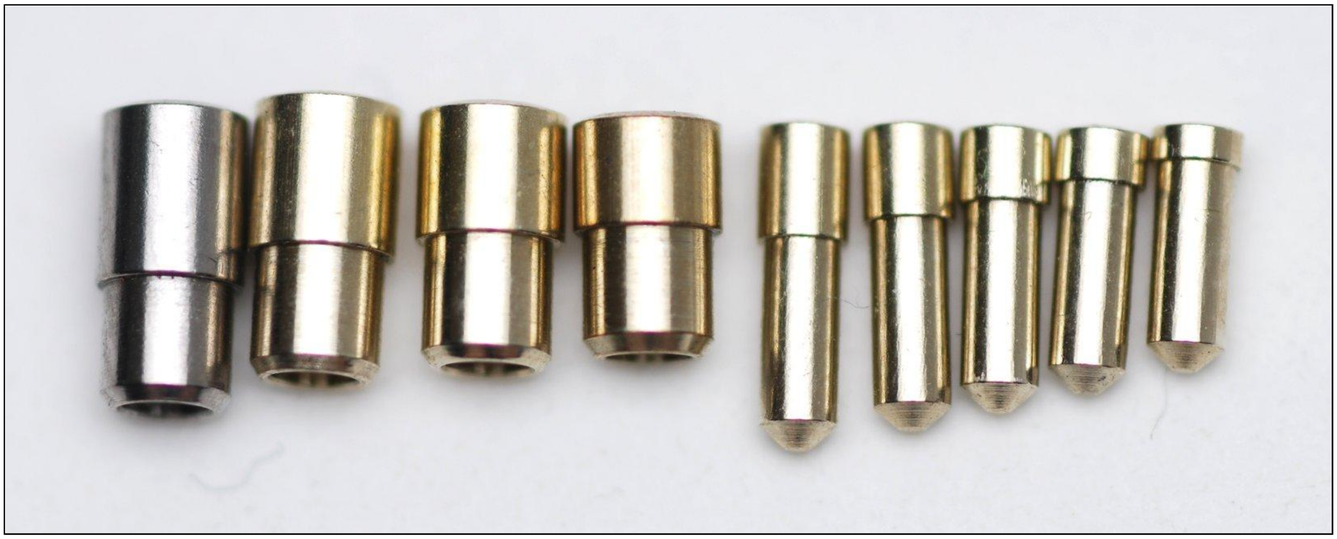


FIGURE 7.14: MT5/MT5+ key pins, sizes A-D (left) and 1-5.

Master keying of the pin-tumblers is provided in the form of master wafers and solid key pins similar to those used in the Classic and Interactive (Figure 7.15). Traditional (non-telescoping) driver pin are used with solid master key pins and can be combined with master wafers for extended master keying.

The sidebar sliders may also be master keyed to provide complex master keying solutions. Slider masters may be in the form of multiple true gates or an extended true gate that spans to adjacent gate positions (Figure 7.16). There are two shapes of master sliders; one that has the slanted edge and another that is flat. Anti-picking false gates are not available on all of the slider masters due to the lack of surface area on heavily mastered sliders.

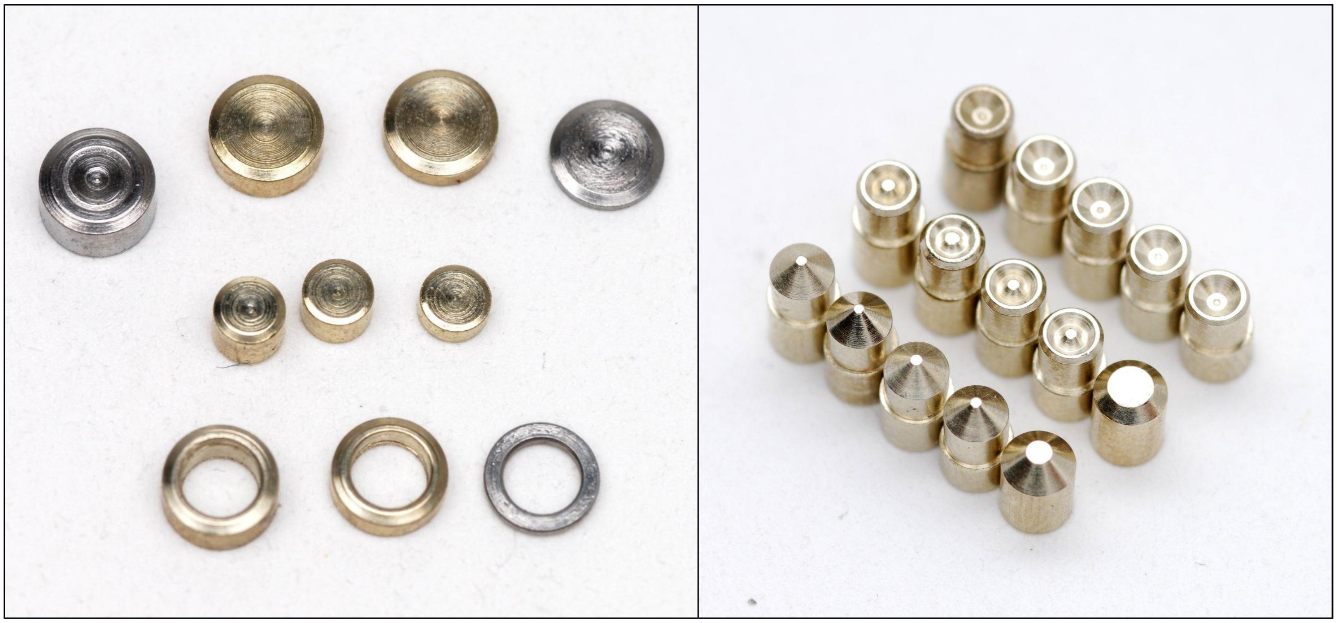


FIGURE 7.15: MT5/MT5+ master pins, both wafer (left) and solid non-telescoping varieties.

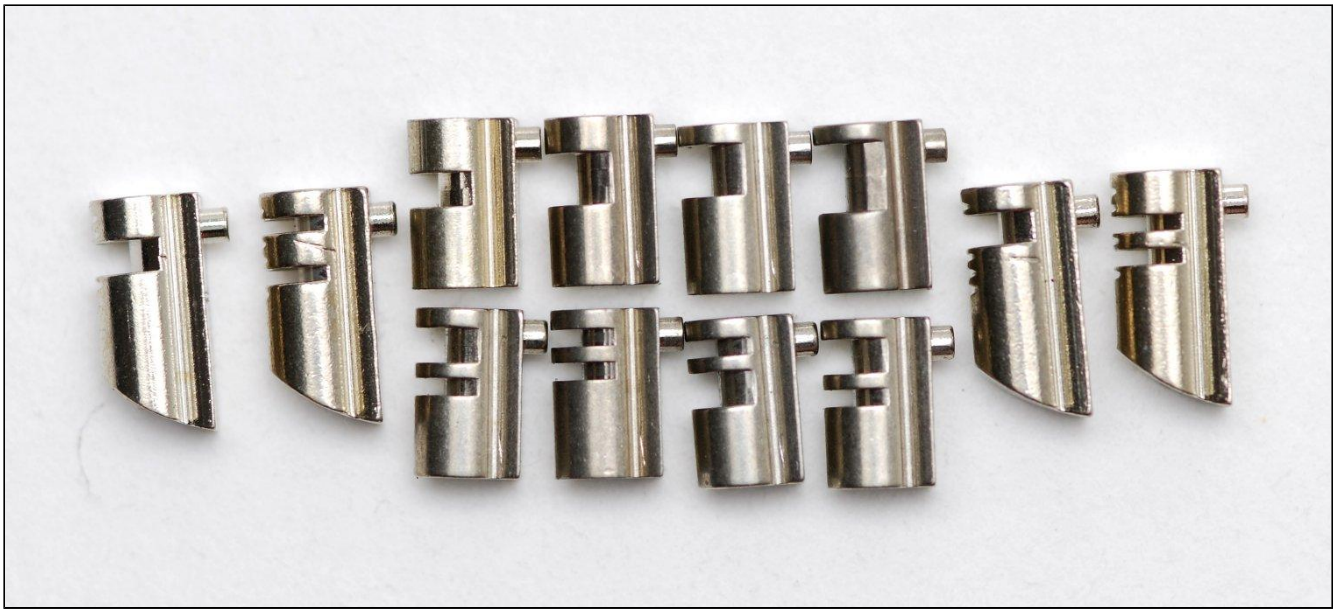


FIGURE 7.16: MT5+ slider master keying, both extended and multiple true gate varieties.

With no master keying the MT5+ provides 4,437,053,125 key differs. This is comprised of the 1,419,857(17^5) telescoping differs and the 3,125 (5^5) sidebar differs. The MT5 has 1.42 million theoretical differs due to the lack of a sidebar. With so many options for master keying, what is the difference between master keying via the sidebar, using solid pins, or using telescoping wafers? Combined, all of the options allow for very large and complex systems. Individually, what a specific installation should depends on their security requirements and their budget.

Like previous models, the MT5/MT5+ can be bitted in various orientations (Left-Up, Right-Down, etc.). Warding on the keys for both MT5 and MT5+ are somewhat unique when compared to other Mul-T-Lock models. Like the restrictions for the Interactive's moving element, MT5/MT5+ keys cannot have warding down the center of the key because of the Alpha spring. Warding is instead reserved for the sides of the blade where the telescoping pin and sidebar bitting are located (Figure 7.17). Warding on the sidebar track cannot be so deep that it affects the track's ability to position the sliders.

One profiling technique that is *not* used in Mul-T-Lock models (to my knowledge) is a progressive profiling feature. In this type of system, the tip of the key will have additional material removed to accommodate more aggressive warding in the back of the lock. Other ASSA-Abloy locks use this, particularly the Abloy series of disc-detainer locks. All Mul-T-Lock models are capable of this type of warding, though I suspect it is not available (or limited use, if it is available) due to high manufacturing costs.

Note: In the Abloy progressive profiling is greatly simplified both in manufacturing and assembly costs by using profiling discs which are easily stamped out.

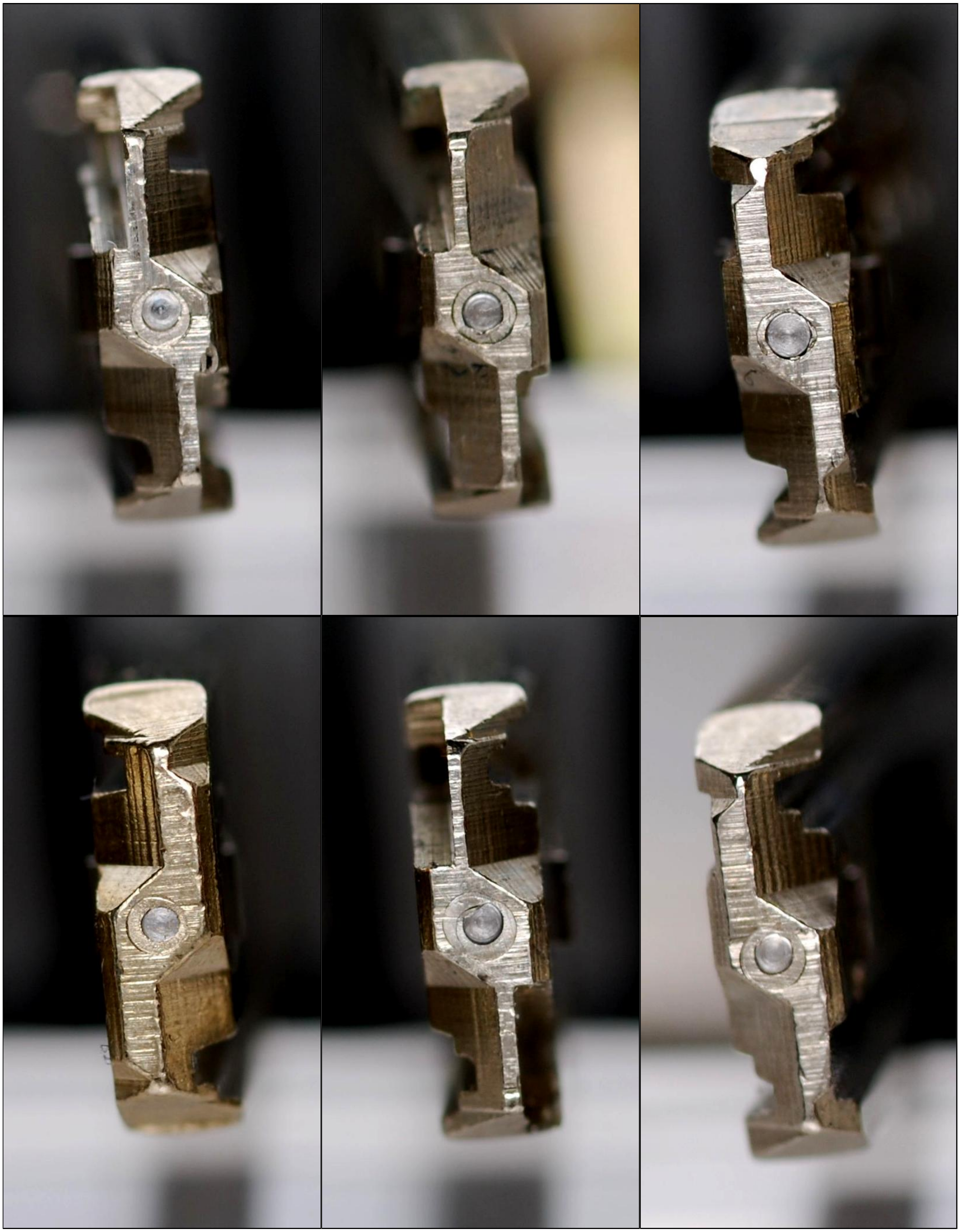


FIGURE 7.17: Six different MT5/MT5+ key profiles.

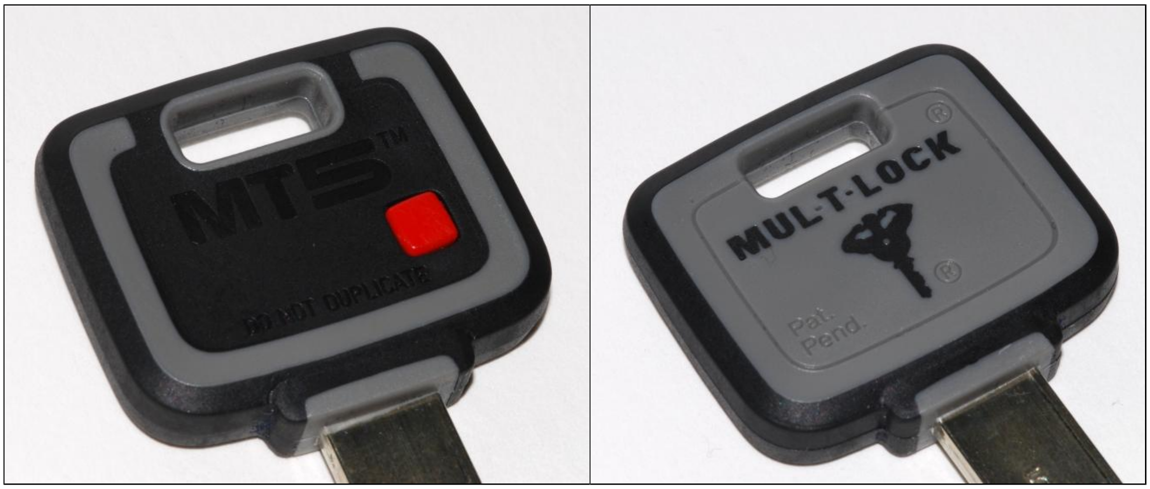


FIGURE 7.18: Front and back of the MT5/MT5+ key bow.

The MT5/MT5+ use one type of key bow and it is unique to these models (Figure 7.18). This key bow is visually distinct and is slightly fatter than previous models. The key bow does not specify if the key is for an MT5 or MT5+ lock, but an examination of the sidebar bitting can clear this up. As you can see, keys are marked "Patent Pending" so a date for patent expiration on MT5/MT5+ keys is currently unavailable. The red square is a user-changeable identifier to spot the correct key without resorting to trial and error.

Anti-Forced Entry

The MT5/MT5+ provides the same anti-forced entry components as previous models. In addition, a ball bearing is included below the bottom steel rod (mirroring the one above), and an anti-drill disc is placed in the face of the lock (Figure 7.19). In the case of the MT5+, the sidebar provides additional resistance against many forced entry techniques.

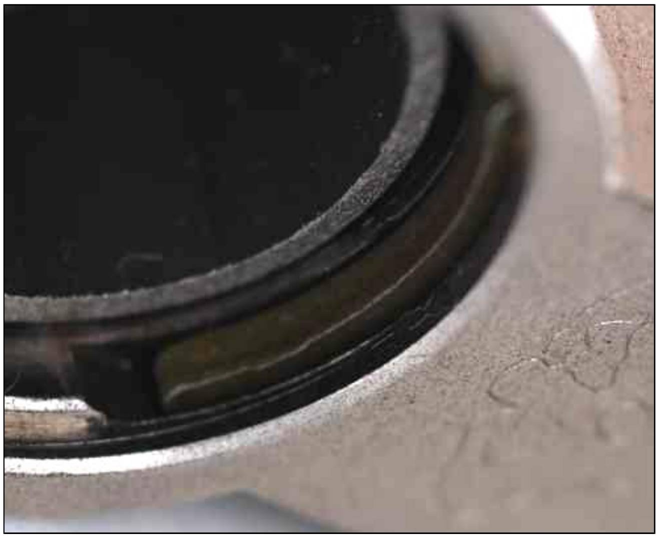


FIGURE 7.19: Anti-drill disc placed in the MT5/MT5+ cylinder, above the plug.

Conclusion

From a purely mechanical standpoint, the MT5+ is the best Mul-T-Lock cylinder to date. It offers a wide variety of protections against both destructive and non-destructive entry techniques. The MT5 is an interesting change, but I don't consider it too different from the Interactive. If you're planning on upgrading, I recommend going straight to the MT5+.

The Alpha spring is interesting but it operates on the same principles as the Interactive moving element. The static position and size of the Alpha spring pins is a little strange, but with the lock being so new Mul-T-Lock has plenty of time to improve the design. Key control is quite high considering the Alpha spring. In the case of the MT5+, a wide variety of key differs is available between sidebar, telescoping pins, and warding styles. The regular MT5 has a high number of key differs, but lack of sidebar makes this a bit dubious.

That's it for the discussion of Mul-T-Lock models. In the next section we'll discuss various attacks against each generation of Mul-T-Lock model, as well as design upgrades and varieties provided by Mul-T-Lock to resist each attack.

8. Security Analysis

A telescoping system is functionally equivalent to a traditional pin-tumbler lock. From a security standpoint, many non-destructive compromise techniques are harder to do. Mul-T-Lock is not the first or only company to provide telescoping pin-tumblers, but they have made many improvements to telescoping systems and dimple locks, in general.

This section will evaluate the strength of Mul-T-Lock systems against a variety of common attacks. Due to the similarity of the Mul-T-Lock models I'm going to categorize by attack rather than by lock model. In each section we'll go over how different models stack up against an attack, vulnerabilities that may exist or previously existed, and how Mul-T-Lock models have evolved to deal with these problems.

Unfortunately, I don't know every trick in the book, and this is a section that I could use much help on. If you have any correction or additions please contact me! Contact information is available at the start of this paper.

Security Ratings

All Mul-T-Lock telescoping locks have earned one or more security ratings. A security rating is a way for consumers to know what level of security to expect from a lock. In the same way that beef is rated Grade “A” by the USDA, locks have grades which define what attacks they resist and for how long. All security ratings are given in time rather than absolutes. For example, a lock may be rated to resist lockpicking for at least 10 minutes, and forced entry for 15 minutes.

Having a security rating does not imply that the lock is “high-security”, just that it passed whatever tests the specific rating requires. This has been a source of confusion lately, especially when we consider UL 437, a popular lock security rating from Underwriter's Laboratories. Many people associate UL 437 with “high-security,” but there is really nothing that makes this so. As Marc Tobias likes to say, it is just a “high-er” security standard.

Mul-T-Lock models have received ratings from Underwriter's Laboratories (UL), American National Standards Institute (ANSI), European Committee for Standardization (CEN), VdS Schadenverhütung GmbH (VdS), and Stichting Kwaliteit Gevelbouw (SKG). Their UL 437 certification is the most notable as far as US ratings go. The Hercular deadbolt series also have ANSI Grade 1 locking mechanisms.

Unfortunately, the exact wording of many standards are not publicly available and are quite expensive to obtain (UL 437, for example, is currently $490 USD). See Lockwiki's Security Ratings page for a listing and descriptions of some of the American standards and ratings.

Forced Entry

Resistance to forced or destructive entry is a primary concern for all locking systems. Forced entry is by far the most common method of entry, and, if successful, is often the fastest and cheapest way to defeat a locking system. Mul-T-Lock systems use a variety of mechanisms to prevent forced entry, detailed in earlier sections, but some tools and techniques can be used to quickly compromise the older Mul-T-Lock Classic and Interactive systems.

Wendt, a German locksmith tool company, make a pulling screw that is effective against a variety of Mul-T-Lock cylinders. It works by being screwed into the keyway, then extreme pulling force is applied to pull the lock out of its mounting.

Multipick Service, another German locksmith tool company, offers a drill bit that claims to go through an entire Mul-T-Lock cylinder in about a minute. They have a video of this on their website, but they make the fatal error of splicing cuts rather than keeping the film running. Like this, we can't confirm that it actually took one minute, only that the clock at the top says so. I'm willing to give them the benefit of the doubt but encourage them to put up a new video which includes assembly of the lock (to verify all components are present), and to not splice the clips.

Lockpicking – Classic & Interactive

In terms of covert entry, lockpicking is the most well known and respected skill an attacker can have. Resistance to lockpicking tools and techniques have become increasingly important to the reputation of a lock since the early 1800s. In modern day, a lock's security is heavily based on whether or not it can resist lockpicking, sometimes generalized as "manipulation." While key bumping makes the headlines lockpicking is still the most tried and true way of opening any lock in the world given the correct tools, time and, most importantly, skill.

All five pin Mul-T-Lock systems have a total of 10 pin pairs when we consider inner and outer pins. While a ten pin lock sounds challenging, in truth the Mul-T-Lock is two five pin locks. Think of it this way: inner pins cannot separate at the shear line before outer pins. The outer pins being at the shear line is (mostly) independent of the position of inner pins. This means the lock can be picked by first attacking the outer pins then inner pins.

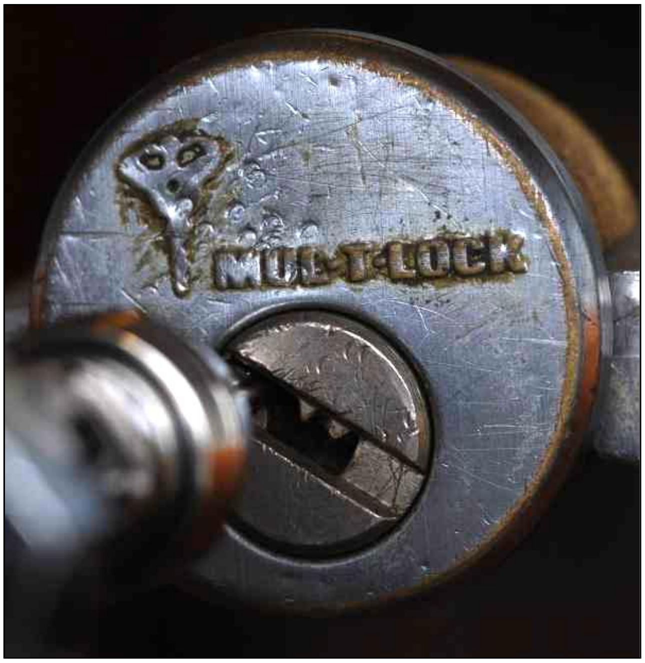


FIGURE 8.1: A Mul-T-Lock Classic fully picked.

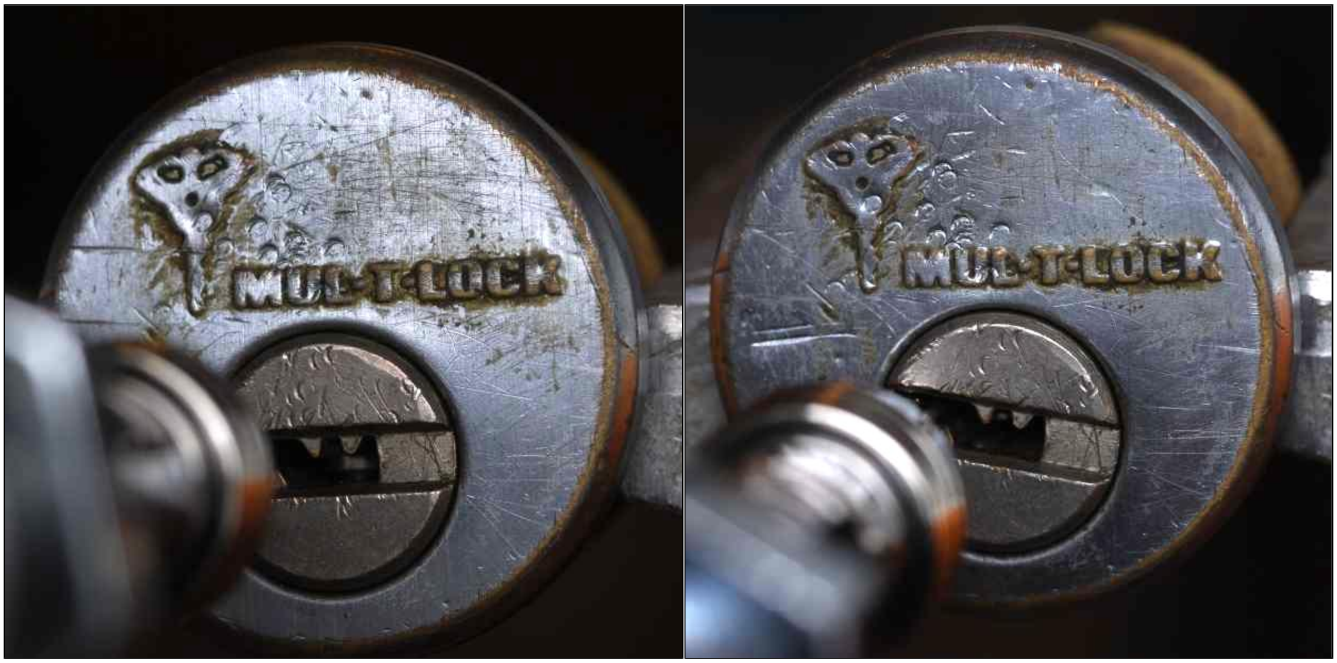


FIGURE 8.2: A Mul-T-Lock Classic in the normal (left) and partially picked (right) positions.

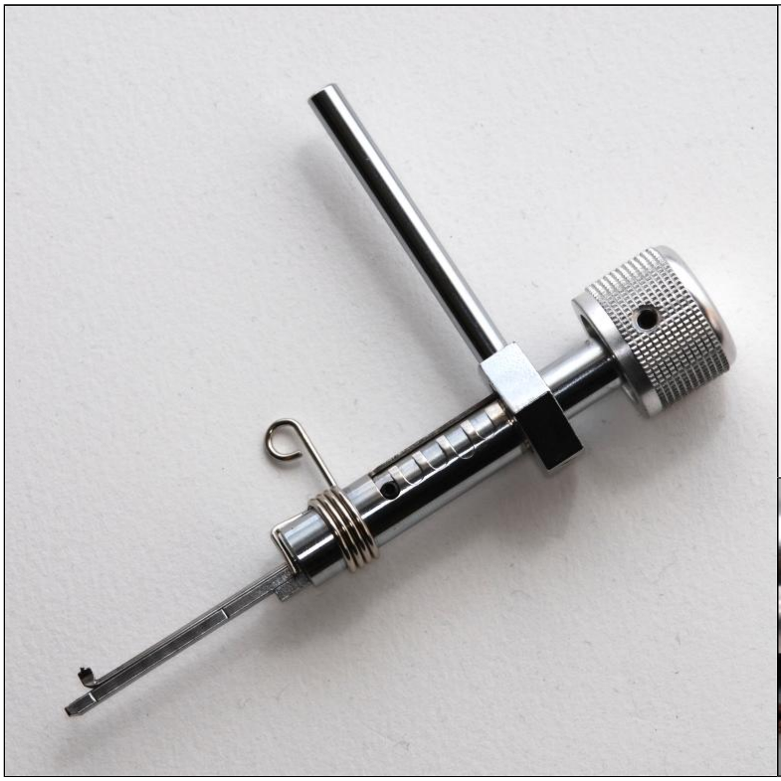
How does an attacker know when to pick the inner pins? When the outer pins are picked the cylinder rotates slightly, more so than the false set of a security pin (Figure 8.2). From here, the attacker can move to the inner pins, and, for the most part, the lock becomes a five pin dimple lock. Picking of the inner pins is very simple. Matt Blaze explains this phenomenon well:

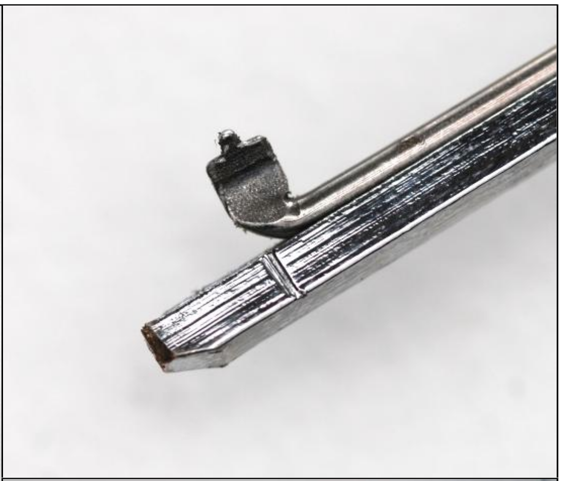
"However, because of the angle at which the inner upper pins are trapped, this should be a much simpler task than ordinary lock picking. In particular, the inner pins can apparently be set in any order (or simultaneously); they all bind at once and over-setting is prevented by the severe angle at which the upper pins are held."

- Matt Blaze, "*Notes on Mul-T-Lock Locks*" (www.crypto.com)

Several locksmith and convert entry supply companies provide picking tools for Mul-T-Lock systems. Wendt produce two sets of Mul-T-Lock picks, both of which resemble traditional dimple lockpicking tools with pointed tips. Multipick Service also sell various Mul-T-Lock picks. Again, sets are traditional dimple picks with slight modifications. The Souber and GOSO dimple pick sets are also effective against Mul-T-Lock systems but aren't designed or marketed for this purpose specifically.

Traditional dimple or pin-tumbler picks can also be used but they take more skill to use. The main problem with traditional picks, and those sold by the companies listed above, is that they can get stuck between the inner and outer pins. When this happens it takes a considerable amount of fiddling to get the pick out. In many cases tension must be released to remove the tool, forcing the attacker to restart the picking process.





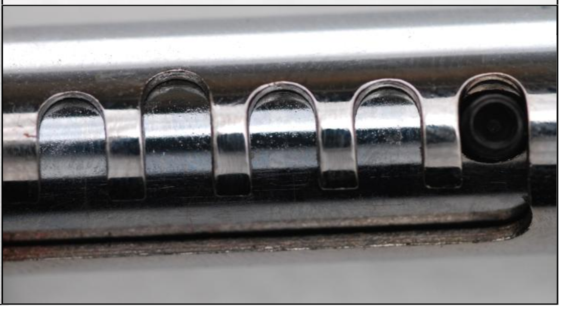


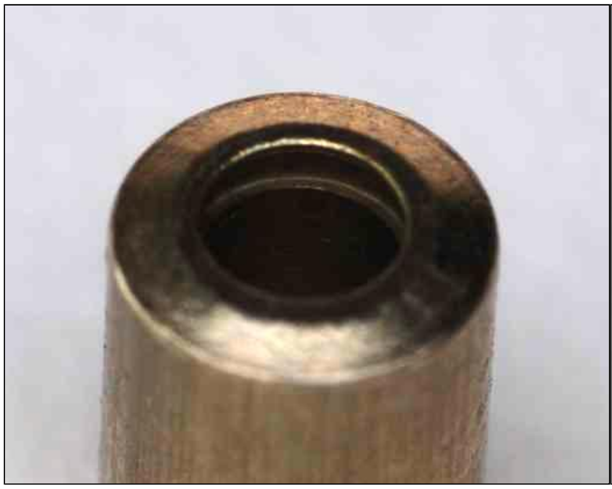
FIGURE 8.3 (Left): The H&M Mul-T-Lock picking tool (Right-Up).
FIGURE 8.4 (Top right): Close-up of the ward track and pick tip.
FIGURE 8.5 (Bottom right): Close-up of the tool's pin channels.

The Mul-T-Lock picking tool that has gained the most popularity is produced by a Chinese company called H&M Tools. The tool is distinct and does not resemble the traditional dimple picks sold by other companies (Figure 8.3). It is extremely effective in picking Classic and Interactive cylinders when compared to traditional tools. Many companies resell the H&M tool; prices range from $75 USD to $600 (!) USD. Shop around!

The tool is inserted on the leftmost ward (in a Right-Up lock) in the plug and is tip-stopped by the cam of the lock. The pick itself sits on a ledge of the tool (Figure 8.4) and is rotated with the large knob at the end of the tool. Tension is applied through a bar that can be placed on either side of the tool.

The tool is calibrated so that it lifts pin stacks only when the working end is directly beneath them. It does so through the use of small channels that indicate which pin stack you are working on (Figure 8.5) and how high you are raising the pins. The second chamber is extended to account for Interactive pin sizes. Being tip-stopped, the tool works in both four and five pin locks without re-calibration. In addition, the tool does not get stuck between telescoping pins due to the shape of the working end.

In order to combat lockpicking Mul-T-Lock made a variety of improvements to their locks. Widespread use of serrated outer driver pins is effective in deterring casual picking, but a medium to highly skilled attacker should have no problem with these. Additionally, inner driver pins can be lightly spooled. On their own they offer a minimal defense, but are combined with outer key pins that use counter milling (Figure 8.6). When tension is placed on the cylinder the inner and outer pin serrations hook together to frustrate picking attempts. Some pins with counter milling also have a serration on the bottom of the outer pin (Figure 8.7). My guess is that these are an anti-decoding mechanism similar to the rings on Medeco pin-tumblers.



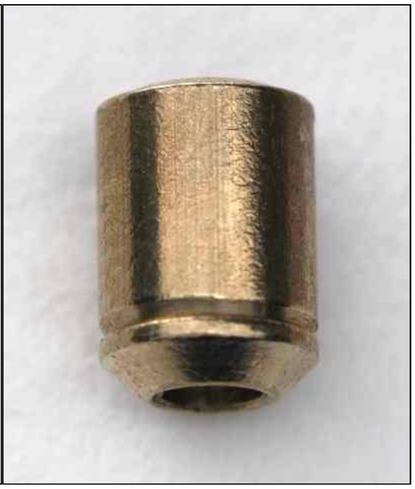


Figure 8.6 (Left): An outer key pin with counter-milling, used to frustrate lockpicking.
Figure 8.7 (Right): Some counter-milled pins have a serration at the bottom of the pin.

Lockpicking – MT5/MT5+

In 2009, I wrote *"As far as I know, there are currently no ready-made picking tools for the MT5/MT5+ cylinders. [...] it is only a matter of time before something is developed."*

The locksmith and locksport communities did not disappoint! Over the last few years many talented people have focused their efforts on attacking the MT5+ using very creative techniques. A number of vulnerabilities have been found with the MT5+, particularly attacks against the sidebar to downgrade the lock to a standard 5 pin telescoping lock. The normal MT5 is basically an upgraded Interactive cylinder, so I will not discuss picking it.

The first vulnerability is a sidebar torsioning technique discovered independently by European and American researchers. On MT5+ European profile cylinders there is a small hole at the face of the lock which is the extension of the groove the sidebar sits in (Figure 8.8). From here a probe can be inserted to bind each slider against the sidebar sequentially without rotating the plug. When a slider is properly positioned the sidebar will slightly retract, allowing the probe to move in further and bind the sidebar against the next slider. This makes the task of picking the sliders extremely easy. The false gates provide no protection against this attack because the true gate is the only position which allows the sidebar to retract enough to move the probe forward.

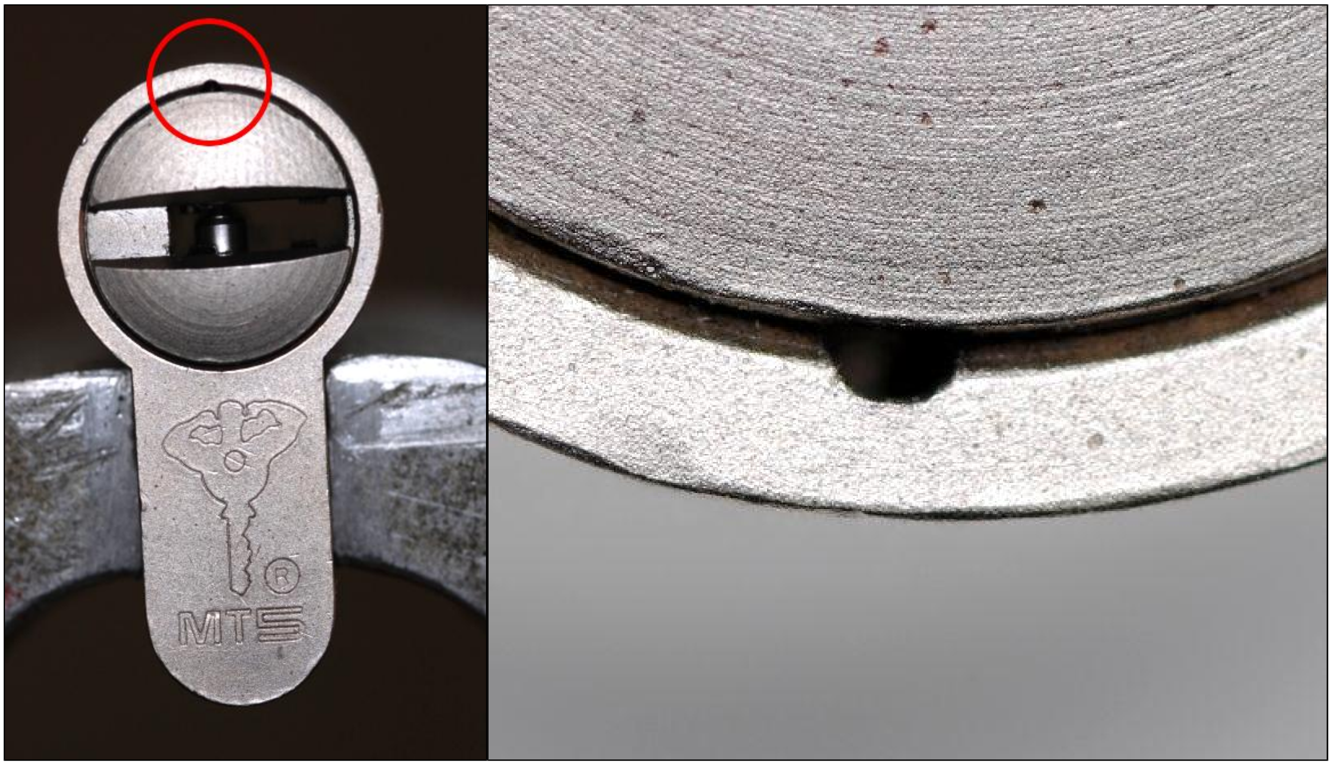


FIGURE 8.8: Normal and close-up views of the extended sidebar slot on European profile cylinders.

What is most useful about this technique is that the probe can be left inside the sidebar slot to lock the slider in place. This allows an attacker to focus on the telescoping tumblers without worrying about the sliders moving out of place. It's my understanding that Mul-T-Lock has since fixed this vulnerability but I cannot confirm it.

Another attack, discovered by Jord Knaap of The Netherlands, uses vibration to bypass the sidebar. In this attack, light torsion is applied with the use of a partial key. It can be a key with both bitting surfaces removed or with a valid telescoping bitting. In either case, a Dremel with an lopsided polishing tool is used to apply vibration through the key, moving the sliders until their true gates are properly positioned under the sidebar.

In both cases the sidebar is disabled and the lock is downgraded to the normal MT5, with only the Alpha spring and the telescoping tumblers to pick. An attacker who can pick an Interactive can easily pick the telescoping tumblers of the MT5/MT5+.

Manually picking the sidebar is more difficult than the above techniques, but it is of course possible. Being located on the bottom of the plug, horizontal to the ground, the position of the sidebar has an interesting effect on picking. Unlike other slider-based sidebar locks (see: EVVA 3KS, Scorpion CX-5), gravity does not affect the position of MT5+ sliders. In short: when picking the MT5+, torsion can be released and sliders will not move. This is also the reason why Jord's attack works so well; sliders don't fight gravity during vibration.

Michaud Attack

Early versions of the Mul-T-Lock Classic and Interactive were vulnerable to an attack discovered by Eric Michaud (TOOOL USA) in 2004. Dubbed the “Michaud Attack,” he found that inner pin-pairs could be raised to lift the outer driver pins, allowing all outer pins to be easily picked via over-lifting.

Inner pins could be raised and they would carry the outer driver pins (Figure 8.9). Once high enough, the cylinder could be rotated to trap all outer driver pins above the shear line. From there, picking the inner pins is easy, as discussed earlier. The original tool that Eric created was similar to a comb pick, which lifted all inner pins at once. A more ideal version of the tool works similar to the Sputnik lockpicking tool where each pin stack can be lifted individually.

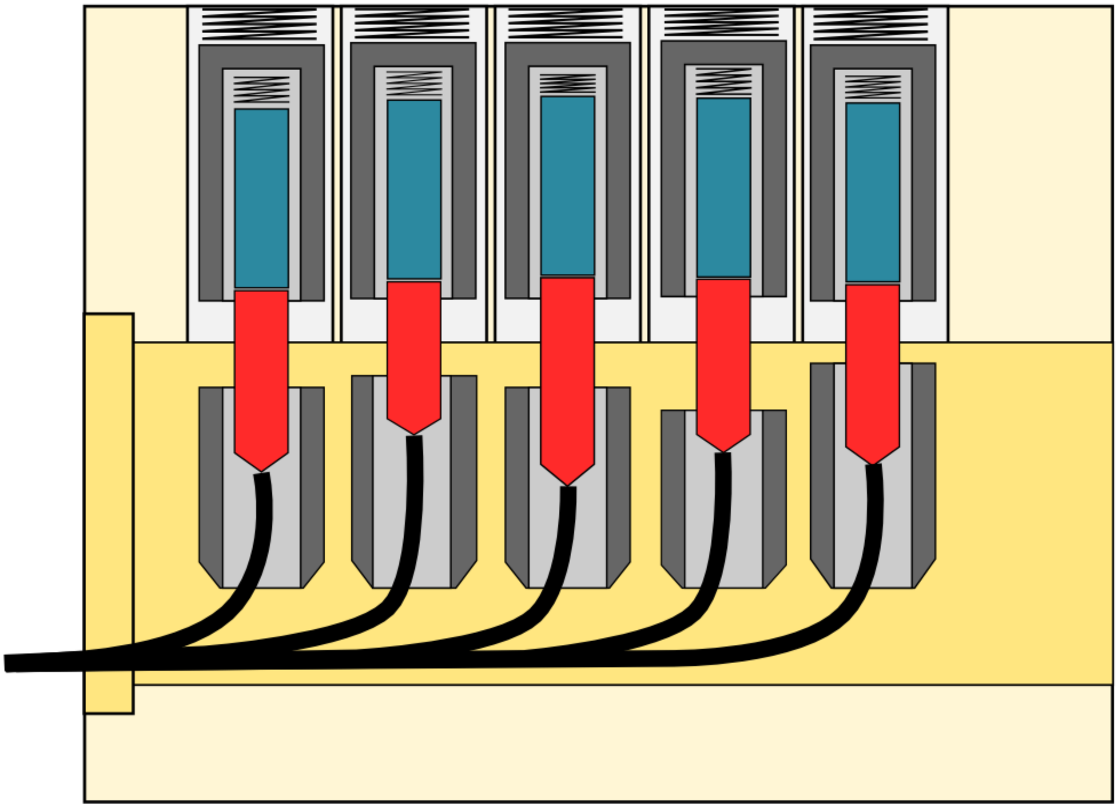


FIGURE 8.9: Using inner pins to lift outer driver pins above the shear-line.

Mul-T-Lock has since fixed this problem, but there are still many locks installed that are vulnerable. Interestingly enough, Mul-T-Lock's fixed their design by using the recommendation of Eric Michaud and Matt Blaze. Their idea was to make a hole in the top outer pin that allows the inner pin to push through when it is all the way at the top (Figure 8.10). Inside the lock, this prevents the outer driver pin from being raised to the top of the chamber through the use of the inner pins. Use of solid key pins in master keyed systems (see Section 4, Master keying) also prevents the Michaud attack on all pick stacks at the expense of pick-resistance and key differs.

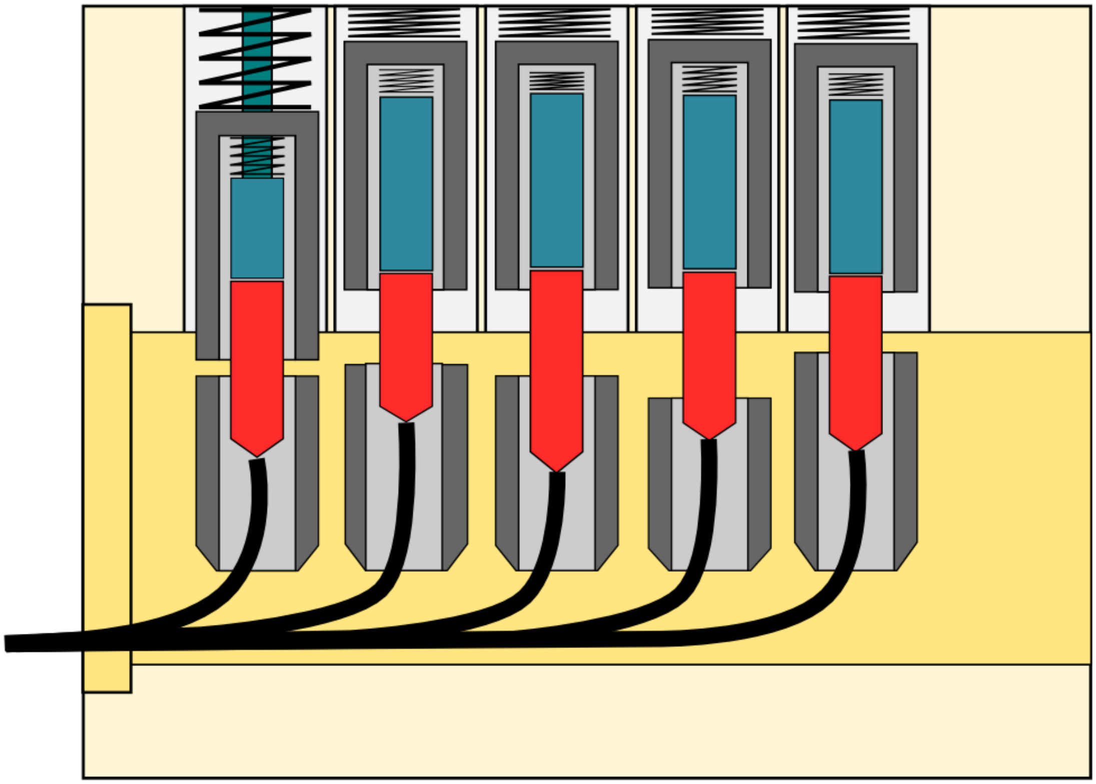


FIGURE 8.10: Pin 1 uses a protruding inner driver pin, which stops over-lifting if it is long enough.

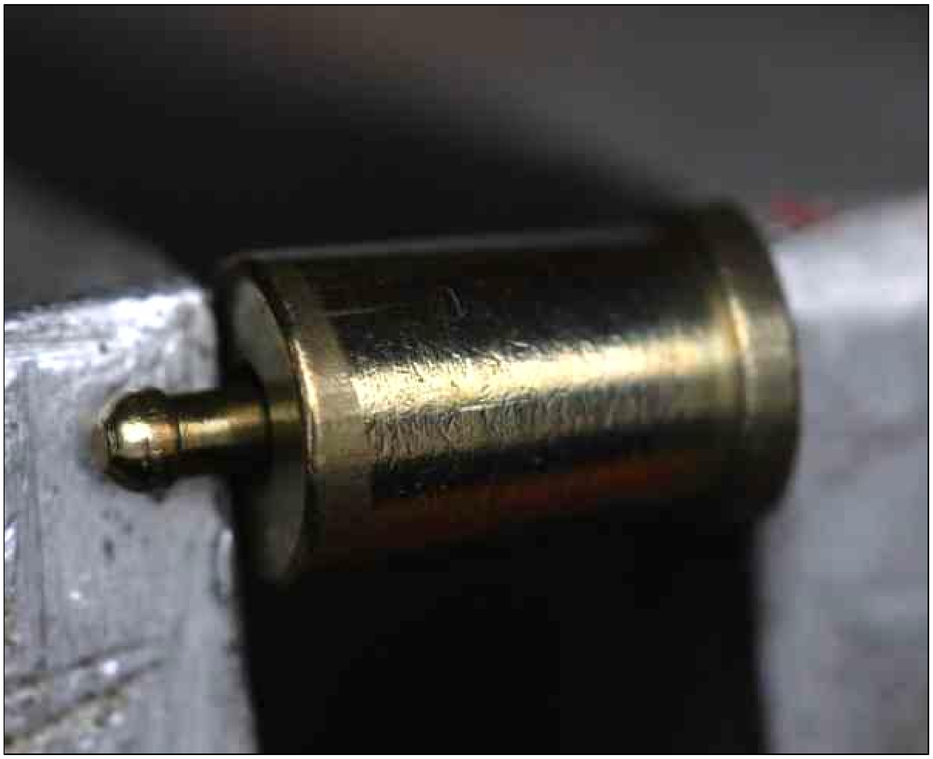


FIGURE 8.11: Modern style “nippled” driver pin, common in almost all new Mul-T-Lock cylinders.

Key Bumping

Key bumping is a covert entry technique where force is applied to a modified key to cause pin-tumblers to split at the shear line. Whether or not Mul-T-Lock models can be bumped is a subject of much debate. After the media frenzy on bumping in 2006, Mul-T-Lock released a press statement (24 May 2007). In short, they claim all videos online are done by people that are not using proper cylinders; they've been modified in some way to make bumping possible:

"*Not a single one of these supposedly successful bumping attempts was performed with a non-treated Interactive Mul-T-Lock cylinder. Mul-T-Lock's bump-resistant Interactive cylinders, as they are assembled in our factories and distributed throughout our network of authorized professional dealers are not susceptible to this type of attack.*"

While I understand Mul-T-Lock's apprehension about admitting they have a (potential) problem, I don't agree that every video is a hoax. I can't point out real versus fake, but I can say I've bumped and witnessed bumping of both Classic and Interactive cylinders without "treated" components. In any event, this is still disputed. The universal Mul-T-Lock bump key seems to be elusive, as sometimes cylinders are difficult to bump. My guess is the complexity of bumping 10 pin stacks at once; timing, force, and a properly cut bump key all play a role.

Obtaining the proper key blank is a concern in bumping. This isn't too hard for the Classic, especially now that the patent has expired, but with the Interactive we need the correct keyway profile *and* moving element. This may be challenging.

The normal way to obtain a key for a target lock, if available directly, is to just buy a lock that has the same keyway profile. We can't always do this with the Interactive because we have to consider the moving element. In my experience, the Silver (S) element is the most popular. Most online vendors sell the Gold (G) element on all cylinders (others may be available upon request). This leaves the Black (B), which is surprisingly hard to find. All of this is coupled with needing the correct keyway profile and the inability to casually observe the keyway profile of Interactive locks. While none of this stops the act of bumping itself, they all make obtaining the information to successfully bump the lock more difficult.

Finally, we consider the MT5/MT5+. If we agree that the Classic and Interactive can be bumped then I see no reason that the MT5 (without sidebar) couldn't also be bumped. With the Alpha spring in a static position and shape, and keyway warding that can be visually decoded, the MT5 doesn't offer the same level of security through obscurity that the Interactive does.

The MT5+, however, is almost certainly not bump-able unless the attacker can obtain a key with the proper sidebar code. In *Key Card Attacks* portion later in this document I discuss one method of creating bump keys for MT5+ locks: bypassing the security controls of Mul-T-Lock's own key machines.

Moshe Dolev, one of the founders of Mul-T-Lock, holds a variety of patents for bump-resistant pin-tumbler designs. Of these, Mul-T-Lock chose to implement a pin type they refer to as the “Split-D” pin (Figure 8.12). The Split-D is a modified outer key pin that uses two parts. Each fit into one another, not unlike the traditional outer/inner pins, and claims to prevent bumping attacks. The logic is that kinetic energy is not transferred properly to the outer driver pin, preventing it from separating at the shear line. I have not had access to these for testing so I cannot comment on their effectiveness.

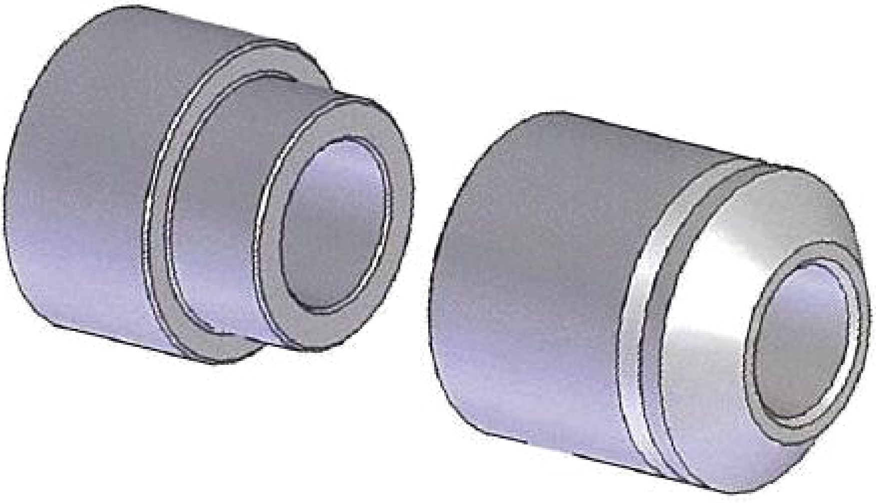


FIGURE 8.12: Mul-T-Lock Split-D type outer key pin, for key bumping resistance.

Some of the Mul-T-Lock press releases also claim that mushroom security pins protect against bumping, but this is not terribly accurate. While they protect against premature tension on the cylinder, most bumping attacks put tension on the cylinder only after it has been struck with a bump hammer. Regardless, the light tension used on the bump key is probably not going to engage mushroom tumblers to the point where they can effectively prevent bumping.

Mul-T-Lock also note their interlocking (counter-milled) pins may resist bumping, but I don't fully agree with this for the same reasons as the mushroom pins.

At the moment I feel that the Classic, Interactive, and MT5 models *without* the Split-D components can be bumped, but I cannot comment on the universal nature of their bump keys. The MT5+ may not be bump-proof in the truest sense, but it is as close as most pin-tumbler locks can expect to get.

Impressioning

Impressioning is a covert entry technique used to open and make a working key for a lock. It is surprisingly effective and easy to learn but how it affects Mul-T-Lock systems is unclear. There are two types of impressioning: copy and manipulation.

Copy impressioning makes a direct copy of a key by making a mold or impression in a medium such as clay, wax, or silicon. With the mold we can casting a working key for the lock. As we discussed in previous sections, this is most effective against the Classic, but the Interactive and MT5's moving elements defeat this technique. This technique could still be used (against all models, and indeed almost every lock in existence) to decode the bitting and sidebar codes.

Manipulation-based impressioning uses a blank key to gather information from the lock itself, a hybrid of lockpicking and decoding techniques. In a normal pin-tumbler, we bind a blank key against the components to make marks on the blank. With these, we know where to file to produce a working key. With a telescoping system, and a dimple key, this is problematic.

With lockpicking we must pick outer pins then move to inner pins. In the same way outer pins need to be impressioned first. Doing so without letting inner pins leave marks is hard, to say the least. Another major problem is making the actual impressioning cuts. Due to the telescoping pins we would need to make outer cuts without touching the inner area. This is fine for a skilled machinist but problematic to do by hand. In both cases it is time consuming.

I developed a method for impressioning Mul-T-Lock Classics using inexpensive materials and common hand tools. If you look at a Classic key, you'll notice a small part of the key touches the pins. Rather than fabricating Classic blanks I decided to make a small piece of brass that simulates *only* the bitting area (Figure 8.13). It is just over 1 mm thick and ~2.5 mm high.

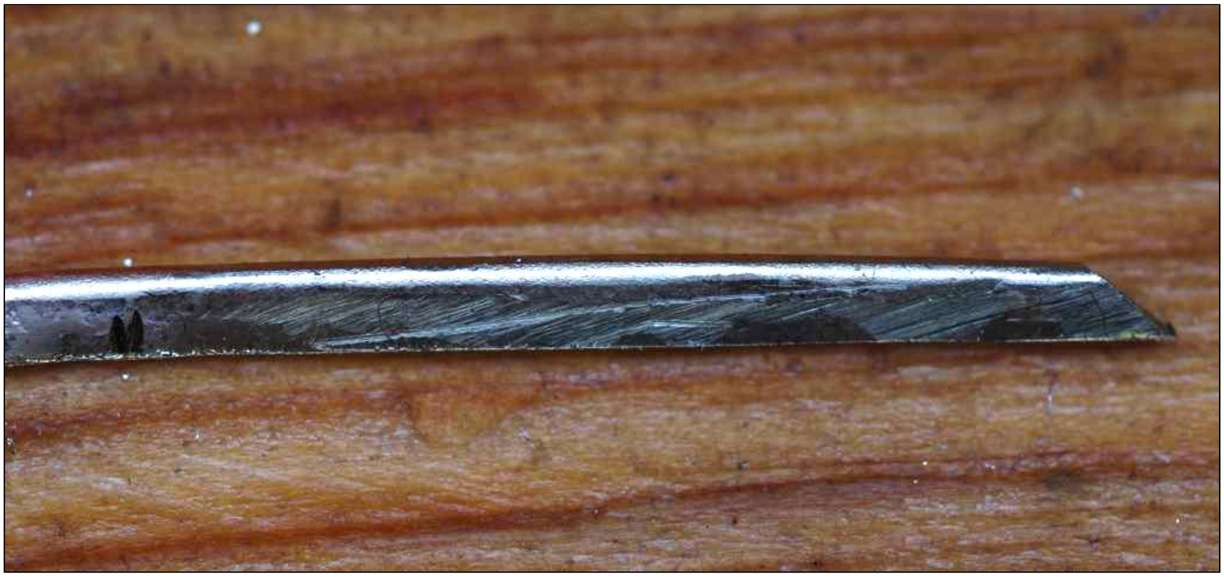


FIGURE 8.13: Mul-T-Lock impressioning tool, made out of brass.

The tool is inserted between the bitting wards and a separate tension tool is used. Methods of obtaining marks are the same as traditional impressioning. The tool is removed once outer pins are impressioned and the cylinder rotates. Normal picks or the H&M tool are used to quickly pick the inner pins. You could continue impressioning, of course, but it takes much longer than picking the inner pins manually. Additionally, large inner pins leave as little as 0.47 mm of material on the tool. This decreases the strength of the tool and may cause bending or breaking.

Early attempts to make impressions were successful but a telescoping system leaves a considerable number of marks. In addition to inner and outer pins, pin chambers also bind against the tool. This is troublesome because I wasn't sure where to file. I moved to a UV-based system, making it easier to find marks as well as identify what made each mark (Figure 8.14).

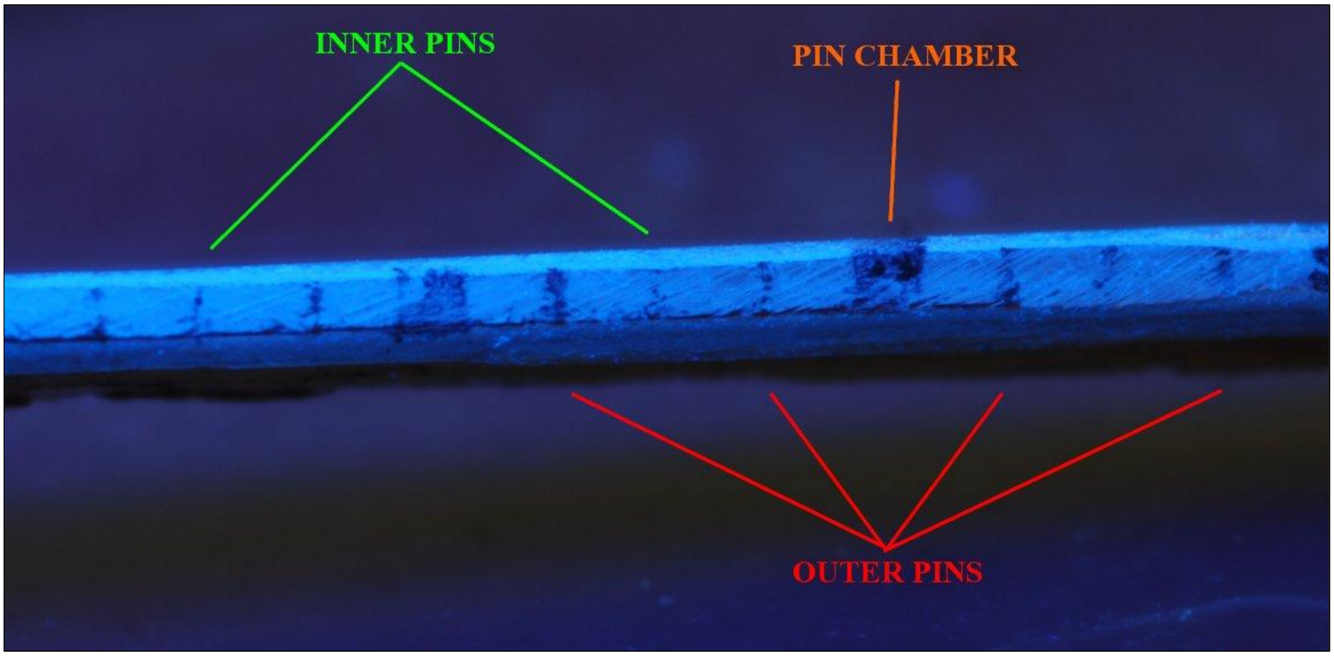


FIGURE 8.14: Impressioning marks on the tool, viewed under UV light.

Aside from the ability to clearly see marks with UV ink, the main advantage is making the impressioning cuts. With the key in a non-dimple arrangement it is much easier to file where marks are. Avoiding the inner pins is easy because you can just file around them (Figure 8.15).

With extremely low pins it is helpful to file at an angle to prevent the tool from breaking easily (a common dimple impressioning trick).

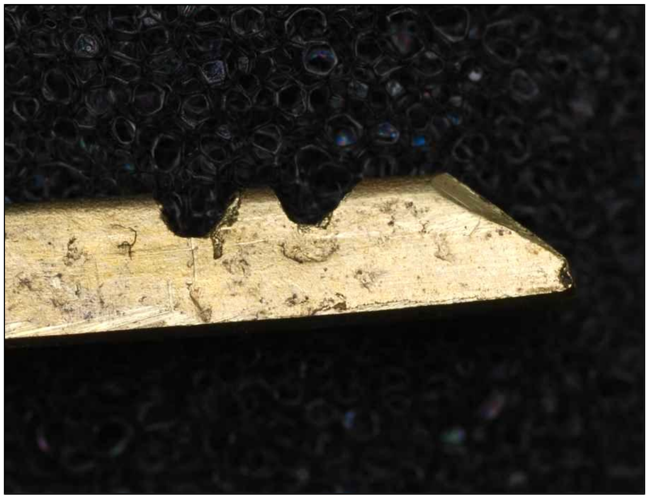


FIGURE 8.15: Tool after the first round of filing.

Pressure-responsive impressioning may also be possible. With this technique a soft, malleable material (such as foil, lead, or soft wood) is used to quickly impression the lock. Many modern dimple locks are vulnerable to this type of attack, but the telescoping pins are again a problem. At this time I have not seen a Mul-T-Lock impressioned this way, but it seems plausible.

Falle-Safe offers an impressioning tool for Mul-T-Lock systems. I believe this is a progressive key system but I have not been able to get a better description or see one in person. Please contact me if you have more information! Contact details are available at the start of the paper.

Decoding

Decoding is a class of attack that aims to figure out the bitting pattern of lock either through examining or manipulating the lock or a working key. With the information gained from decoding a working key can be made by hand or with a key cutting machine. Decoding is somewhat ambiguous, in general, so it is hard to pin down exactly what decoding techniques the Mul-T-Lock may be vulnerable to.

With the H&M picking tool, marks could be made to decode the lock while it is being picked. It would be neat if the tool came like this, but it is not too hard to do by hand.

A mold taken of any Mul-T-Lock key could be decoded to determine the bitting and sidebar patterns for the lock. Mul-T-Lock does not use any bitting codes on factory original keys that could be used to decode them, but the associated key cards do. Classic and Interactive key cards use direct codes, including the full keyway profile (See Appendix A).

Falle-Safe offers a picking and decoding system they claim work with Mul-T-Lock systems. I believe it is just a traditional dimple pick set and a standard lever type decoder. In the tool's description Mul-T-Lock is grouped in a category with other locks and it basically says, “some may be harder to pick and decode than others.” What this means for Mul-T-Lock specifically is unclear. I have not had access to this system in person so I cannot comment further.

Electromechanical Attacks (CLIQ & SynerCLIQ)

At Defcon 17 (Aug 2009) Marc Tobias and Tobias Bluzmanis discussed vulnerabilities in the Mul-T-Lock CLIQ originally discovered by Jord Knaap of the Netherlands. Shortly after, Barry Wels and Han Fey of TOOOL NL demonstrated these attacks at Hacking at Random (HAR) 2009. Given that the CLIQ is used in various government and high-security installations around the world, namely airports in the USA, the security implications are enormous.

Of particular concern, the sidebar and electronic authentication could be bypassed through a variety of attacks. This means covert or surreptitious entry is possible without any visible evidence on the lock or in the electronic audit trail. Remember the CLIQ is powered by the key, thus attacks that open it without needing to power the lock internals bypass the audit trail.

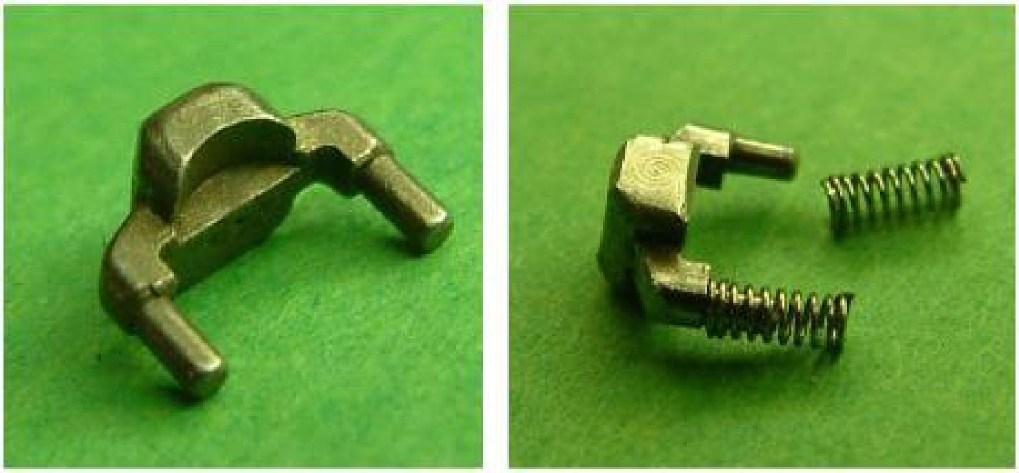


FIGURE 8.16: Design variations in the Mul-T-Lock CLIQ sidebar. (Image courtesy of Barry Wels)

The attacks against the CLIQ allow the sidebar to be retracted, making traditional forms of covert or surreptitious entry possible. Though similar, each technique uses a different method of compromising the sidebar. The first uses magnetism to bias the sidebar into the plug. In this video you can see Barry Wels demonstrating the magnetic attack with a tool dubbed “the devil's ring”. The second technique uses vibration via a lopsided Dremel bit to retract the sidebar. You can also see Barry demonstrating the vibration attack.

In both cases the compromise of the sidebar defeats the electronic portions of the lock, basically turning it into an expensive Mul-T-Lock Interactive. The videos demonstrate opening the lock via a key with the correct mechanical bitting but incorrect (or nonexistent) electronic portion. Remember that once the sidebar is retracted traditional lockpicking and decoding techniques can be used, as well. The difference between the two types of compromise is that a working mechanical key would be surreptitious (in general), but we could still find forensic evidence of most lockpicking and decoding methods.

The researchers also showed that there are varieties in the sidebar design (Figure 8.16). There are two generations of Mul-T-Lock CLIQ. Marc Tobias and Tobias Bluzmanis claim to be able to defeat newer generation CLIQ locks, but specific details on the vulnerabilities have not been made publicly available.

Both attacks show that sophisticated electronic locks are subject to attack. Just because a lock incorporates electromechanical components does not guarantee its security, nor does it detract from the fact that it is still, at heart, a lock that is opened by mechanical components. Too often do people proclaim electronic locks as “the next big thing” without considering the implications of traditional physical attacks in *addition* to potential electronic attacks. The CLIQ is a perfect example of this in the real world. Traditional attacks are still effective against it, despite its advanced auditing and key control capabilities. Hopefully more information will be available in the future. Particularly, I think it will be interesting to see how Mul-T-Lock improves the CLIQ to protect against these attacks.

Key Card Attacks

All of the credit for this section goes to Babak Javadi of TOOOL USA for his hard work with MT5/MT5+ key cards. I helped, marginally, by providing a piece of the puzzle, discussed below.

Another interesting area of Mul-T-Lock research is key control, particularly the ability to make any key with MT5/MT5+ key machines. When a person buys one of these locks they get a key card which is used to get more keys made (Figure 8.17). The key card owner can bring it to a Mul-T-Lock dealer to have their keys duplicated. Unlike other key machines, the MT5/MT5+ key machine will only create keys for a given key card. If a user buys a lock, then loses the key card, the locksmith is unable to make them additional keys. Thus, the ability to make any key is useful for both locksmiths and attackers.

The cards themselves are standard hi-coercivity, three track magnetic stripe cards. If you take a key card and run it through a magnetic stripe reader, you will get something like the following:

```
%ML06000000C6D1JIDVNN00000002CP6P6VC2CO6ICI?
;1234567890123456789012345678901234567?
```

Only the first track of the card is used (the numbers on track 2 are just filler) and it contains information on the key profile and bitting. This particular card has a header of: `ML06000000C6D1JIDVNN0000000`, followed by 15 bytes which define outer pin, inner pin, and finger pin bittings (Figure 8.18).

OP1	IP1	OP2	IP2	OP3	IP3	OP4	IP4	OP5	IP5	FP1	FP2	FP3	FP4	FP5
2	C	P	6	P	6	V	C	2	C	O	6	I	C	I

FIGURE 8.18: 15 byte array of Outer Pin (OP), Inner Pin (IP), and Finger Pin (FP) bittings.

However, knowing that Mul-T-Lock pins are named A-D and 1-5, 2PPV2-C66CC-O6ICI is obviously not a valid bitting code. These cards use a simple substitution cipher to mask the direct bitting. By correlating the known key bitting with the key card data Babak figured out the mapping to the real bitting of CAABC-21122-41323 (Figure 8.19). The original work with these cards was done with a set of ten key cards that had the same key profile but different telescoping and sidebar bitting information. The bitting information was decoded, but the header information remained a mystery. Enter your fearless author; I took a look at the card data and was able to decode the header and the rest of the cipher alphabet.

DIRECT	A	B	C	D	1	2	3	4	5
ENCODED	P	V	2	8	6	C	I	O	U

FIGURE 8.19: Decoding table for encrypted MT5/MT5+ key card bittings.

The actual encryption is an affine cipher (`a=6, b=15`), a mono-alphabetic substitution cipher. This type of encryption is extremely insecure because it can be cracked by solving a simultaneous equation once you know two plain text characters. In our case we have much more than that from the valid bitting codes. It is also possible to solve this type of cipher by hand just by looking at letter distribution. When you compare the plain text and cipher text alphabets, a pattern emerges. The cipher alphabet is being chosen by starting at A = P, then skipping six characters. If you lay out the plain text and cipher alphabets side by side, this is easy to spot:

```
CIPHER: PQRSTUVWXYZ123456789ABCDEFGHIJKLMNO
PLAIN:  A     B     C     D     E     F
```

The full cipher alphabet is as follows:

```
PLAIN:  ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
CIPHER: PV28EKQW39FLRX4AGMSY5BHNTZ6CIOU17DJ0
```

With the full alphabet we can decrypt the header portion of the card listed earlier:

```
CIPHER: 06000000C6D1JIDVNN00000002CP6P6VC2CO6ICI
PLAIN:  010000002186938BXX0000000C2A1A1B2C241323
```

We now have all the information available on the card; 2186-938-B-XX is the keying code, and CAABC-21122-41323 (rearranged) is the bitting information. This information allows anyone to make a copy of any MT5/MT5+ key, or to use the machine to create non-standard bittings, such as that of a bump key.

The key machines themselves are extremely expensive, in the tens of thousands of dollars. This rules out casual attacks, but a friendly or unscrupulous Mul-T-Lock dealer can assist. It's also possible that a locksmith would be tricked by a rewritten card. Let's assume an attacker rewrites a legitimate card with bitting info that they want. They could take this into a Mul-T-Lock dealer and get copies of the key. It's not plausible for the locksmith to determine if a key corresponds to a given key card; not all cards have a direct bitting code printed on them!

Ultimately the key card system fails to provide much security for the actual duplication of MT5/MT5+ keys aside from needing the key machine to facilitate key creation. A more sophisticated implementation would separate the bitting information from the card entirely, or mask it on the card using much stronger encryption. However, both of those approaches could be attacked through software and hardware avenues. While it's a big step forward for key control and a good move on the part of Mul-T-Lock, I think it will be a long time before a “secure” implementation of card-based key duplication is available.

9. Conclusion

Mul-T-Lock is a world leader in locking technology, best known for their telescoping “pin-in-pin” systems. We went over the various Mul-T-Lock models and learned how each works. While they provide increasing resistance to attack over the years, they all use the same basic locking principles, even the newer MT5 models.

In my opinion the normal MT5 is not much of an improvement over the Interactive model; it just moves the floating component to the back of the lock and adds a sixth pin-stack. At the time of writing this it is unclear whether or not the Alpha spring provides the same variety in position and style like the Interactive moving component, but all samples I have seen or examined place the Alpha spring in the sixth pin chamber and don't appear to have alternate bitting styles.

The MT5+ is Mul-T-Lock's best mechanical cylinder to date, offering high pick, bump, and impressioning resistance. The addition of the sidebar is a dramatic improvement over previous models, offering a solid defense against various destructive and non-destructive entry methods.

While older models are not without problems, they are still effective in providing security to the majority of installations. The choice of lock will depend on the type of installation and the security required. In most low to medium security installations the Mul-T-Lock Interactive (and even Classic, in some cases) will do an adequate job of providing protection. Newer models, particularly the MT5+, can provide security even in high security situations. At present, the future of the Mul-T-Lock CLIQ is in question, as the serious security vulnerabilities presented drastically reduce the security offered by the lock. Hopefully Mul-T-Lock will correct these problems in future CLIQ models.

Thank you for reading. I hope you learned from and enjoyed this paper! For more articles on locks, safes, forensic locksmithing, and locksport visit http://www.lockpickingforensics.com.

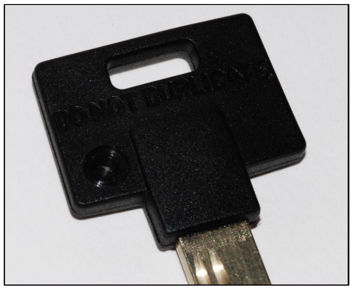
Be sure to keep reading further for various appendices that you might find interesting and useful.

datagram, Fall 2012

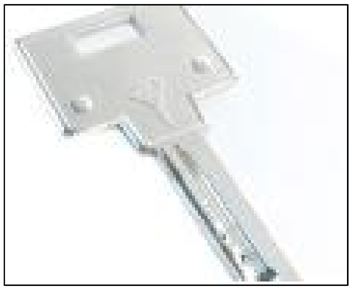
Appendix A: Keying Specifications

Key Bows

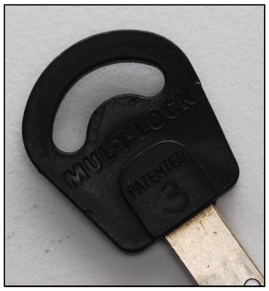
Mul-T-Lock keys follow a simple key coloring and coding scheme to identify the lock model, keyway profile, moving element position, and moving element type (where applicable). The shape and color of key bows can be used to quickly identify the model of the key. Below is a comparison of different Mul-T-Lock key bows:



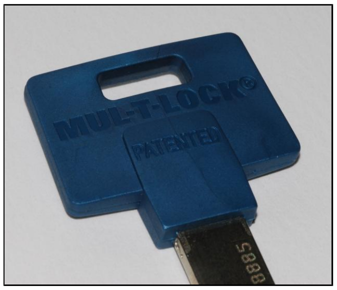
Classic, square plastic (Black)



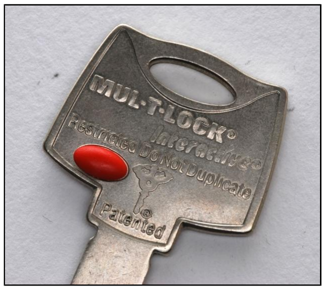
Classic, nickel silver



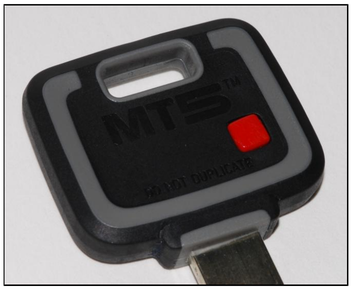
Classic/Interactive, round plastic



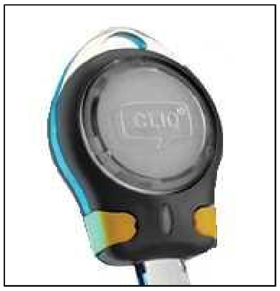
Interactive, square plastic (Blue)



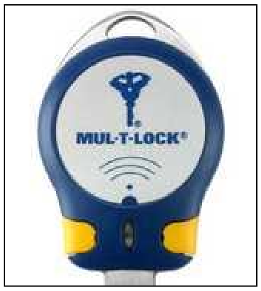
Interactive, nickel silver



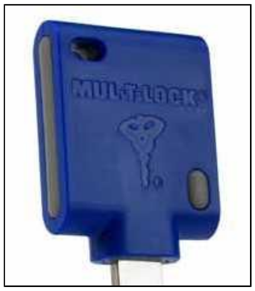
MT5/MT5+, square plastic



Interactive CLIQ, oval plastic



Interactive SynerCLIQ



Interactive SynerKey

Notes

- 3-in-1 Interactive keys are square plastic keys with a green, yellow, or red bow.
- 3-in-1 Classic keys may instead use a black square plastic bow with colored inserts.
- Alternate key bow designs are used in Europe/Israel, but are otherwise rare.

Keying Codes

Mul-T-Lock key codes follow the format of XYYZ. Key codes can be found on the blade, just below the bow of the key. Most codes printed on keys are limited to XYY or YY. Examination of the bitting can determine the Z code, if necessary.

X **Moving element position**:

0	Classic/7x7 (no moving element);
1	Interactive/Integrator first position
2	Interactive/Integrator second position
5	Integrator position 5
6	Integrator position 6
7	Integrator position 7
8	MT5
9	MT5

YY **Keyway profile**

Z **Moving element type**:

C	Classic
S	Silver (uniform heights; Z-0)
B	Black (outer pin higher; Z-1)
G	Gold (inner pin higher; A-0)
M	Integrator Master Profile
P	Integrator Internal Cut Profile
E	Integrator External Cut Profile
7	7x7
A	MT5
B	MT5+

Notes

- Padlocks as usually listed as [KEY CODE]-[PADLOCK CODE]
- The 7x7 and Integrator are non-telescoping dimple locks made by Mul-T-Lock
- This data is not accurate for MT5/MT5+; they have extended key coding information.

Classic/ Interactive/3-in-1 Keying Specifications

Inner/Outer Key Pin Specifications*

Pin Designation		Key Blank Left (Cut Depth)	Pin Length	
Inner	Outer		Inner	Outer
0	Z	n/a (Interactive)	4.75 mm	4.65 mm
1	A	2.40 mm	5.25 mm	5.20 mm
2	B	1.95 mm	5.75 mm	5.65 mm
3	C**	1.45 mm	6.25 mm	6.15 mm
4	D**	0.95 mm	6.75 mm	6.65 mm
5		0.45 mm	7.25 mm	

* Applicable to Classic, Interactive, Interactive CLIQ, and 3-in-1 cylinders
** C and D outer pins may also be of the inverted mushroom style.

Interactive (moving) Component Specifications

Name	Code	Description	Pinning (Outer-Inner)
Gold	G	Convex; inner pin higher	A-0
Silver	S	Flat; both pins equal	Z-0
Black	B	Concave; outer pin higher	Z-1

Master Pin Specifications

Pin Designation		Pin Length	
Inner	Outer (external/dual*)	Inner	Outer (external/dual*)
4		2.00 mm	
3	3	1.50 mm	1.45 mm
2	2	1.00 mm	0.97 mm
1	1	0.50 mm	0.47 mm

- Dual refers to a master pin which provides a uniform shear-line for both pairs of pins. It looks similar to a traditional pin-tumbler master pin. “External” outer master pins refer to the ring shape master pins which change the shear-line of the outer pin stack only.

MT5/MT5+ Pin Specifications

To be added in a future revision.

MT5/MT5+ Master pins

To be added in a future revision.

MT5+ Slider Specifications

To be added in a future revision.

MT5+ Slider Master Pins

To be added in a future revision.

Appendix B: Padlock Naming Conventions

Mul-T-Lock padlock model numbers follow the format of WXXYZZ.

W **Padlock series**:

C	"Heavy duty" (silver; rectangular or square)
E	"Extra-high duty" (black/silver with a colored strip at the bottom)
G	"Medium duty" (silver; square and lightly rounded)
T	"Heavy duty" (silver; round body, sliding bolt, and puck padlocks)

XX **Padlock "size"** (meaning varies):

E/C series	Shackle clearance length (mm)
G/T series	Padlock horizontal length (mm)

Y **Shackle options**:

P	"Popping" shackle
R	Removable shackle
x	Popping/removable shackle (up to consumer)
C	Various shackle sizes available (may be used with other Y options, such as xC/PC)

ZZ **Shackle protection**:

x	Not shrouded
P	"protected" (with shroud)
LE	"low guard" (low shroud)
HE	"high guard" (full shroud)
SP	"shackle protector" (removable black shroud)
SB	"sliding bolt" (self-shrouded sliding bolt)

Therefore, the G44P defines a G series padlock, 44 mm in horizontal length, and with a shrouded/protected shackle. A C13xCx defines a C series padlock with 13 mm of shackle clearance, your choice of popping or removable shackle, varieties in shackle size, and non-shrouded.

Notes

- ZZ is frequently shortened to Z.
- Y may expand to YY if the 'C' option is used (*such as xC, PC*).
- Sometimes ZZ and Y are swapped; look at the table for clarification.
- YZZ is sometimes omitted when browsing online stores or locksmith catalogs.
- Padlocks as usually listed as [KEY CODE]-[PADLOCK CODE].
- Some E series padlocks may also be sliding bolt; it is not restricted to the T series.

Appendix C: Patent Listing

This is a list of all the patents I could find that are assigned to Mul-T-Lock relating to telescoping locks, padlocks, or keys. Some other patents are excluded; key machines, bolts and latches, and automotive patents. If you have any additions or corrections please contact me! At the end of this section are telescoping pin-tumbler locks *not* registered to Mul-T-Lock, all of which are interesting. The original telescoping patents discussed in Section 2 are listed there, too.

US Mul-T-Lock Patents

Patent #	Title	Description
4,142,389	Cylinder lock	1977, Classic cylinder
4,856,309	Cylinder lock	1987, Classic cylinder
5,123,268	Cylinder lock	1990, Classic cylinder with a variety of pin designs
5,267,461	Cylinder guard	1990, Cylinder guard shield, marketed as "Top Guard"
D933973	Key bow	1990, Classic key bow (rounded plastic)
D335253	Key blade blank	1990, Classic key blank
5,331,307	Gear shift lock	1991, Gear shift lock
D342887	Key blank	1991, Classic key blank
D353320	Key blank	1993, Classic key blank
D353534	Key blank	1992, Classic key blank
D353760	Key blank	1993, Classic key blank
5,520,035	Locking apparatus	1994, Interactive cylinder
5,784,910	Locking apparatus	1996, Interactive key blank (206 keyway)
5,839,308	Locking apparatus	1997, Interactive cylinder
D411435	Padlock body	1998, E series padlock (body only)
D411730	Padlock body	1998, E series padlock, shrouded (body only)
D415010	Padlock body	1998, E series padlock (body only)
D422880	Padlock shroud	1998, E series high shroud
D422883	Key bow	1998, Interactive key bow (nickel-silver)
D426138	Padlock shroud	1998, E series low shroud
6,393,876	Padlock	2000, E series shrouded padlock
7,086,259	Pick resistant lock	2000, Telescoping lock with counter-milled key pins
10,593,553	Monitorable lock	2005, Electronic padlock that monitors against forced entry

Israeli Mul-T-Lock Patents

Links are direct to patent PDF files. The Israeli patent site segments the patent document, so the patent # links to the claims and 'D' links to the drawings. There are many patents that are "abandoned" or have not reached the "second publication phase." Some have interesting titles, so I'll try to add these if/when they become available.

Patent #	Title	Description
50,984, D	Cylinder lock	1976, Classic cylinder
59,705, D	Padlock	1980, C series padlock
62,034, D	Covering arrangement	1981, Protective cover for cylinder-based mortise locks
67,607	Key for cylinder locks	1982, Double sided dimple key (no drawing)
80.808, D	Locking device	1986, Padlock and shackle shaped to fit motorcycle tires
83.701, D	Pin-tumbler lock	1987, Classic cylinder
90,211, D	Cylinder lock	1989, Classic cylinder
92,982, D	Cylinder lock guard	1990, Cylinder guard shield
96,954, D	Padlock	1991, C series padlock (with removable shroud)
99,623, D	Cylinder lock guard	1990, Cylinder guard shield, marketed as "Top Guard"
99,696, D	Tamper resistant lock	1991, Tamper resistant Classic cylinder
102,153, D	Padlock	1992, C series padlock (removable shackle)
102,754, D	Cylinder lock	1992, Classic cylinder with key profiling mechanism(s)
103,041, D	Padlock assembly	1992, Padlock used as gear shift lock in automobiles
104,349, D	Locking apparatus	1993, Interactive cylinder
109,263, D	Key head	1994, Interactive key bows
109,351, D	Door lock	1994, Interactive cylinder
110,606, D	Locking system	1994, Classic cylinder with two rows of pin chambers
116,159, D	Anti-tampering lock	1995, Padlock with anti-tamper mechanisms
117,323, D	Changeable lock cylinder and key rotating pins	1996, Mechanically changeable lock cylinder and key rotating pins. (Cool patent)
118,998, D	Cylinder lock	1996, Classic style cylinder with three telescoping pins
119,095, D	Lock housing	1996, T series sliding bolt padlock
122,509, D	Padlock	1997, E series padlock (with low and high shrouds)
129,563, D	Anti-theft apparatus	1999, Transponder key system for automobiles
150,362, D	Pick resistant lock	2002, Classic style cylinder with counter-milled pins

Other Telescoping Pin-Tumbler Locks

Patent #	**Title**	**Description**
593,436	Lock	1897, Telescoping pin-tumbler
917,365	Pin-tumbler lock	1908, Telescoping pin-tumbler / wafer hybrid
1,095,500	Lock	1914, Telescoping pin-tumbler
1,244,304	Cylinder lock	1917, Sort-of telescoping pin-tumbler with “arms”
2,022,070	Lock	1935, Telescoping pin-tumbler
2,158,501	Tumbler lock	1938, Faux telescoping pin-tumbler
2,653,467	Anti-pick cylinder lock	1951, Telescoping pin-tumbler (Michaud attk. immune)
3,869,889	Tumbler mechanism	1973, Telescoping pin tumbler
3,818,732	Cylinder lock construction	1973, Telescoping pin-tumbler *and* tubular lock. (Both are immune to the Michaud attack)
4,760,722	Cylinder lock	1987, Grouped telescoping pin-tumbler (cool keys)
4,996,856	Structure of cylinder lock	1990, Tubular 3-level telescoping lock
5,222,383	Cylinder lock	1992, Cruciform telescoping pin-tumbler
5,894,750	Lock	1997, Odd dimple lock. Possibly basis for Alpha spring?

Please contact me if you find any telescoping pin-tumbler patents to add to this list! Contact information available at the beginning of this paper.

Note: *I realize there are some locks from the early 1800s that are “telescoping,” but these are usually slider based. I am primarily interested in telescoping pin-tumbler locks.*

Credits, Thanks

Many people helped make this paper a reality. In no particular order: Jon King, scorche, Babak Javadi, Deviant Ollam, Eric Schmiedl, stderr, Marc Weber Tobias, Tobias Bluzmanis, mh, Mitch Capper, and Rafi Venner.

It's impossible to thank Jord Knaap enough. Jord has a fantastic talent for opening high security locks. His continued dedication in opening these locks is the reason for many updates to this paper!

Much thanks to Eric Schmiedl for letting me use his fantastic CLIQ photos for Section 5. Eric is a great photographer (and lock picker!); visit his portfolio at http://www.ericschmiedl.com.

A big thanks to Barry Wels for input on the Electromechanical Attacks portion of Section 8. Barry was also kind enough to lend me some pictures from his HAR 2009 presentation.

Han Fey's work with ASSA, DOM, and Abloy was motivational and helpful in deciding how to organize this paper. His articles on high security locks can be found on TOOOL NL's website.

References & Resources

All patents referenced in the history section are available in Appendix C.

A few pictures were used from Mul-T-Lock's site(s), press releases, and promotional material. I considered this “fair use” under United States law, but if you are Mul-T-Lock and you are unhappy about it let me know and I will remove them. The full text of Mul-T-Lock's key bumping press release (discussed in *Section 8, Security Analysis*) is available at: http://mul-t-lockusa.com/newsdetails.asp?newsid=58.

Matt Blaze has an excellent introduction to Mul-T-Lock Classic cylinders on his website: http://www.crypto.com/photos/misc/mul-t-lock/.

LockWiki – lockwiki.com

A collaborative online encyclopedia that focuses on locks, safes, and physical security. Help out and contribute! Lockwiki's Community Portal lists many groups and related sites. Many of the photos in this paper are available under Creative Commons licenses on Lockwiki.

Lockpicking Forensics – lockpickingforensics.com

The first and only website dedicated to forensic locksmithing! More articles are available on the Articles page. Be sure to visit the Links page for a list of related sites. If you are looking for training on locks, safes, covert entry, or forensic locksmithing, see the Contact page.

REVISION HISTORY

v2.0 – 10.11.2012:

- Massive layout changes, many photos retouched or retaken.
- Changed pin references from “top and bottom” to the more universal “driver and key”
- Expanded Michaud Attack section.
- Added information on Mul-T-Lock MT5/MT5+ defeats from 2009-2012, thanks to Jord Knaap.
- Added information on MT5 key card encryption, thanks to Babak Javadi.
- Patent section name corrections, thanks to Rafi Venner.
- Added MT5/MT5+ master keying, key profiling, and key specifications (appendix) sections. This might not make it into the 2.0 version and I'll probably forget to update this sentence.

v1.01 – 01.15.2010:

- Corrections on European ratings organization names, thanks to mh.
- Additional information about Mul-T-Lock history and a historical note on impressioning the Mul-T-Lock Classic, thanks to Rafi Venner.
- Updated CLIQ attack information, thanks to Jord Knaap, Marc Tobias, Tobias Bluzmanis, Barry Wels, and Han Fey.

v1.00 – 07.17.2009 – Initial release