A Review of Security Features in the CX5

By Mow

INTRODUCTION

The CX5 (also known as Scorpion, Scorpion CX-5, or Marks Hi-Security) is a high-security lock consisting of 5-7 shearing pin tumblers and 4-5 unsprung sliders interfacing with a sidebar. CX5 is a South Korean company that also operates in Canada while Marks is an American company that licenses the design. The lock may be branded CX5, CX-5, or simply say Scorpion or MARKS.

CX5 locks are manufactured in many popular formats such as mortise cylinders, rim cylinders, key-in-knob cylinders, Schlage-style large format interchangeable cores (LFIC/FSIC), BEST-style small format interchangeable cores (SFIC), and residential deadbolts. Many of these formats are available with the UL-437 rating and come with several extra security features.

The key to the CX5 is a traditional pin-tumbler key with 5-7 cuts along its edge (depending on format, more on this later), with the extra twist of a sidewinder groove along its left side to interface with the sliders.

CX5 key

The slider-sidebar system and the shearing pin-tumblers are two completely independent locking mechanisms. Both must be set correctly for the lock to open, and during a picking attack they need to be manipulated independently.

When the lock is in the locked state, the sidebar is pushed out of the by two small springs located on the far left and right edges. It sits in a small groove in the housing, and when the plug is turned, it is forced inwards and into the sliders. If the sliders are not correctly lined up, it will be blocked and the plug will not continue to turn.

TECHNICAL DETAILS

Before I delve into the specific design features, I want to enumerate the technical specifications of this lock.

The pin-tumbler portion consists of 10 heights, labeled 0-9. The MACS is 6.

The sliders consists of 4 heights, labeled 1-4. There is no MACS.

The number of possible keys for various formats is detailed below.

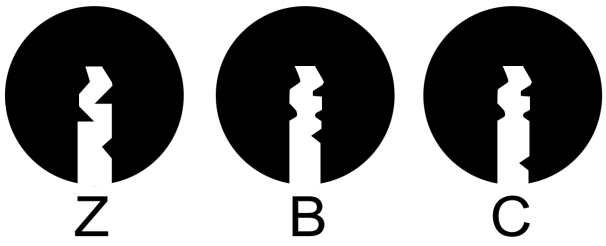
Key combinations

	Pins	**Sliders**	**Valid pin-tumblers**	**Valid sliders**	**Total valid keys**
Standard 5-pin cylinder	5	4	62,948	256	16,114,688
Standard 6-pin cylinder	6	5	562,670	1024	576,174,080
6-pin SFIC	6	4	562,670	256	144,043,520
7-pin SFIC	7	4	5,029,530	256	1,287,559,680

Note that not all of the slider cut combinations are sold; for example bittings like 22222. However, this bitting is technically physically possible, and therefore I am including it. In addition, some of the pin-tumbler keys are bitted like 222222 or 543210, which are typically not used as they can be removed from the lock while the plug is turned given sufficient key wear (pullout keys). These two restrictions limit the usable keyspace, however not significantly.

In addition to the raw number of key combinations, the CX5 uses 3 different keyways, the Z, B, and C, shown below:

CX5 Keyways



These keyways are not cross-compatible in any way, and, as far as I know, multi-section keys do not exist for them. It appears that a multi-section key could be easily produced for the B and C keyways, however again to my knowledge no such key exists.

The pin-tumbler portion of the lock is open to being master keyed. As far as I know, the slider-sidebar portion is not. As well, construction keying is supported for all pin chambers in certain formats.

There are 8 heights of master pin available, with only single-step master pins being disallowed.

There is one height of driver pin.

Depths, spaces, and pin heights are shown below.

Bottom pins

Cut	Height (in)
0	0.166
1	0.181
2	0.196
3	0.211
4	0.226
5	0.241
6	0.256
7	0.271
8	0.286
9	0.301

Master pins

Cut	Height (in)
2	0.030
3	0.045
4	0.060
5	0.075
6	0.090
7	0.105
8	0.120
9	0.135

Top pins

Cut	Height (in)
1	0.177

Cut depths

Cut	Height (in)
0	0.339
1	0.324
2	0.309
3	0.294
4	0.279
5	0.264
6	0.249
7	0.234
8	0.219
9	0.204

Cut spacing

Cut	Space (in)
1	0.246
2	0.402
3	0.558
4	0.714
5	0.870
6	1.026

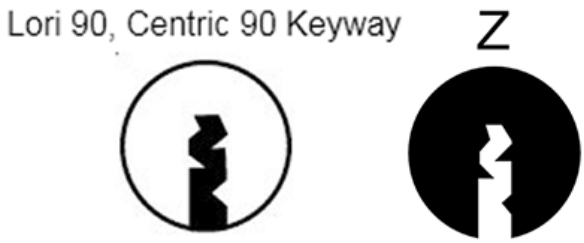
KEY CONTROL

Like the Schlage Primus and ASSA Twin series of locks, the CX5 side milling is cut at the factory and then the regular pin cuts are done by a locksmith. This is a fairly common idea, and allows for exclusivity and key control by restricting distribution of the key blanks of a particular side milling. Tiers of side millings can be established internally by the company. As well, it means that locksmiths need not own any additional hardware over traditional code-cutters to produce keys. In many cases locks ordered by that locksmith will come with the slider-sidebar system pre-installed so they need not even bother with it.

The CX5 offers 5 levels of key control: national, super-regional, region, district, local, and open. Larger areas of restriction are more expensive. Contracts prevent the unauthorized distribution of key blanks.

I cannot comment specifically on how effective the region-based key control is; it seems to be rather well-done on a cursory glance, but that may or may not be the case under more scrutiny.

Specifically, the only issues that I have with their key control is the 'Z' keyway is extremely close to the Lori 90 keyway, for which key blanks are not difficult to obtain (Ilco IL-90, JMA 1614). A Lori 90 blank is essentially a CX5 Z keyway blank with no side milling, leaving keys able to be duplicated using a regular sidewinder duplicator, or, for someone insane enough, a Dremel or other hand tool. I have no idea how this even happened, and I'm not even sure which keyway came first. Either way it is very strange.



Lori 90 keyway comparison

PIN-TUMBLER PORTION

The pin-tumbler portion of the CX5 has 5, 6, or 7 chambers, depending on format. Mortise, rim, and key-in-knob cylinders are available in 5 or 6-pin versions, SFICs are available in 6 or 7-pin versions, and deadbolts and LFICs are available in 6-pin versions only.

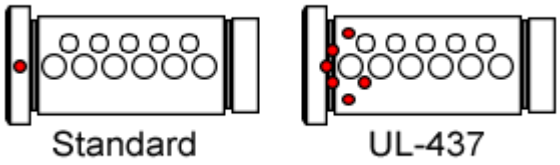
In some of these formats, there is too little room within the bible chambers and the driver pin is partially hollowed out to accept the spring and conserve space:

A hollowed out driver pin

The springs are quite soft and very easy to compress. This is, I believe, to reduce wear on the key caused by friction from the pins.

In the UL-437 rated versions, mortise, rim, and key-in-knob cylinders are only available with 6 pins. In addition, the driver and key pins are made from stainless steel. This provides additional resistance to

breaking or drilling out the pinstacks. Extra anti-drill points are added in front of and between the pin chambers within the plug, as shown below.

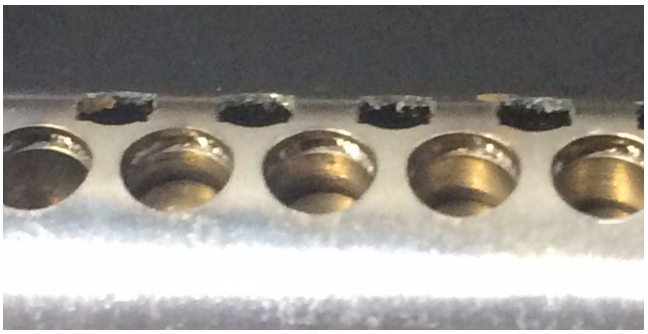


Anti-drill inserts

Note that there are actually some anti-drill inserts that would not interfere with a well-planned drilling attack.

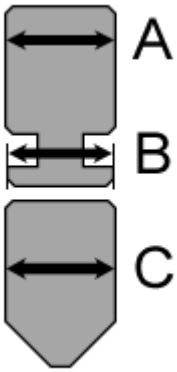
For manipulation resistance, the driver pins are sharply spooled (AKA "gin bottle" pins) and there is matching countermilling within the chambers:

A gin bottle spool pin



Countermilling in the pin chambers

This has the effect of locking the pin up when it is lifted while tension is applied. The sharp tip of the pin will lock into the countermilled chamber and it can be difficult to get it out without dropping previously picked pins. This is not at all a bad mechanic for manipulation resistance; other locks such as the ASSA Twin 6000 use precisely the same idea and are extremely difficult to pick as a result. However, the implementation of this mechanism by the CX5 is flawed. Consider this diagram of a gin-bottle spool with keypin:

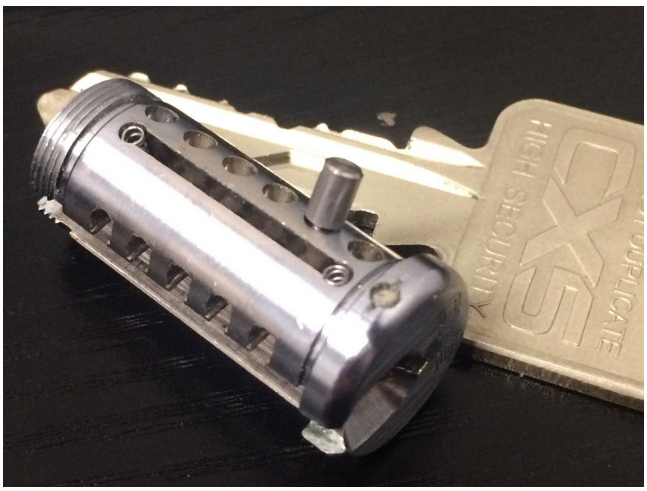


A gin bottle pinstack

To be effectively pick resistant, A and C should be exactly the same and B should be smaller than both. The ASSA Twin and 600 series of locks do precisely this. If A was larger than C, overlifting attacks would be able to set the driver pins while allowing the key pins to fall back into the plug. If A was smaller than C, oversetting the pin would not be possible and picking would become trivial.

In most CX5 locks, A, B, and C are all the same diameter. This generally makes them slightly easier to pick than ASSA's implementation as the tip of the pin has lesser ability to snag the countermilling, but it does not actually compromise the security of the lock. Reducing their diameter and adjusting the countermilling to match would improve the pick resistance of these pins.

In fact, for fun I swapped out a CX5 driver pin with an ASSA driver pin and attempted to pick it. Indeed I believe it is slightly more difficult to pick. However, I quickly noticed that when the plug is turned, the reduced diameter tips of the ASSA pin will fall into the holes for construction balls. This may be part of the reason that CX5 opted to keep B the same size as A and C. If they were to change this, the design of the construction keying feature would need to be changed as well (perhaps to donut-shaped master pins with corresponding holes?).



An ASSA gin bottle pin stuck in the construction keying holes

However, there is a more severe issue. As I mentioned earlier, in some formats the driver pins are hollowed out on top to accept the springs. In whichever way they manufacture these pins, it has the side effect of slightly enlarging the pin diameter. I suspect that the gin-bottle lip is cut last, as B follows the diameter of A. Thusly A and B are both larger than C. This is very bad for pick resistance, as it means that overlifting attacks can bypass the pin-tumbler portion of the lock entirely. There

exists a sweet spot where all of the driver pins will stay up inside the bible, but pushing the keypins up into the bible will cause them to be pushed back down without binding. This is the essence of the overlifting attack.

I do not believe this issue is present in older locks branded 'Scorpion'. I have seen it work in all locks branded 'CX5' that contain the hollowed driver pins.

One other issue exists in the pin-tumbler portion of the lock. In some cases, it seems that a 0-cut keypin (max lift) will not lift the driver pin above the shear line:

A driver pin entirely inside the plug

This can cause problems in a master key system, where a key bitted with a 9-cut (zero lift) will open a 0-cut (max lift), with the driver pin sitting entirely inside the plug. This allows springs near the shear line, meaning they may become caught and mangled inside the chamber. The same may happen if the lock was opened via picking or bumping.

Speaking of bumping: the pin-tumbler portion appears to be quite vulnerable to bumping. The pinstacks are not at all balanced (only one height of driver pin), and the springs are quite weak. The main defense against bumping is that the slider-sidebar mechanism will still prevent the lock from opening if the side milling is not correct. In any practical situation the mere existence of a secondary locking mechanism will quickly stomp out bumping attempts.

To counteract these vulnerabilities, the CX5 could allow for multiple heights of driver pins and proper pinstack balancing.

SLIDER-SIDEBAR PORTION

The slider-sidebar portion of the lock consists of 4-5 sliders depending on format. Specifically, only SFIC cylinders, both 6 and 7-pin variants, come with 4 sliders.

The sliders and sidebar are both made of chrome-plated brass. A hardened anti-drill insert is installed at the 9 o' clock position in the plug to protect the sidebar from being drilled out.

The sliders are left springless to reduce wear on the side milling of the key due to friction. In addition, the chambers the sliders sit in have rounded walls in order to minimize contact. This has the effect of reducing friction even further and lowering the chances of the sliders sticking due to debris or cold temperatures.

Slots the sliders rest in (drawing top left)

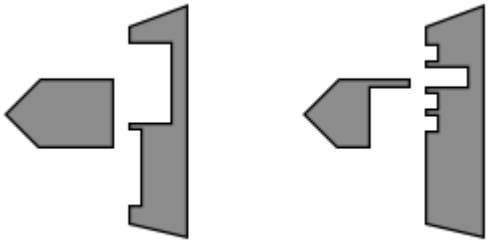
In the UL-437 rated versions of the CX5, the sidebar is made out of steel to increase resistance to forcing and drilling.

For manipulation resistance, the sliders have false gates:

A slider with true and false gate

A particular flaw with the slider system exists in SFIC cylinders. They are available in both 6 and 7-pin variants, and a feature of SFIC is a 7-pin master key can open both 6 and 7-pin cylinders while a 6-pin key cannot open any 7-pin cylinders. As a result, 7-pin keys cannot be fully inserted into 6-pin cylinders and will stop before the shoulder strikes the plug face. However, the 4 sliders are always all the way at the front of lock and therefore a 7-pin key will only interact with 3 out of 4 sliders in a 6-pin lock. To remedy this, the CX5 manuals recommend removing the front slider and shifting the remaining 3 one space toward the front. This obviously weakens the effectiveness of the slider system in SFIC systems.

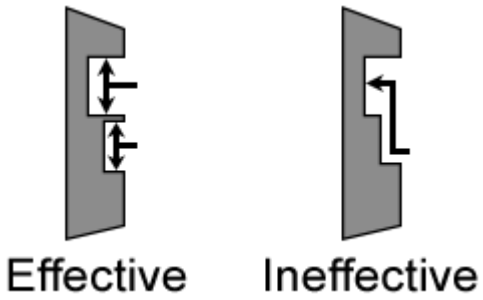
However, the sliders also have several other flaws in their implementation. First, take note of these two sidebar designs:



Two different sidebar designs

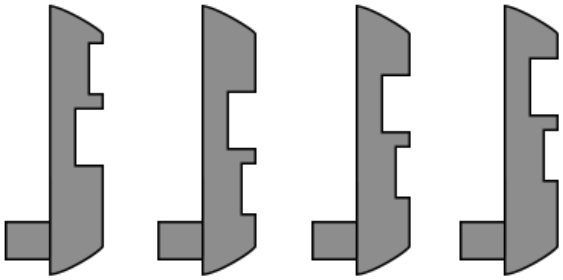
The CX5 is more similar to the design on the left. This design is very limiting: it allows for relatively few possible cuts on the slider and it means there is very little room for false gates. False gates must have a 'wall' between them and the true gate. Locks such as the ASSA Twin, ASSA Desmo, EVVA Dual, EVVA DPI, Mul-T-Lock MT5+, Ikon WSW, Sargent Signature, and probably many others all follow the design on the right. Many of these designs use sliders with 4-5 false gates alongside the true gate.

Only a few other slider-sidebar locks use a design resembling the left, such as the Yale Superior or Millenco Magnum.



Two different false gate designs

The CX5 has a relatively small number of slider positions at only 4, compared to 5 in the ASSA Twin for example. Each slider in the CX5 has one false gate alongside the true gate. There is not enough room on the slider to vary the position of this false gate. As such, there are only 4 possible sliders in total:



All types of slider (to scale)

Note that this picture shows what I believe to be a newer design of false gates. I have seen images from service manuals which show a completely different design of false gate, however it appears to be too narrow to interact with the sidebar, so perhaps it would be more fitting to call it a serration:

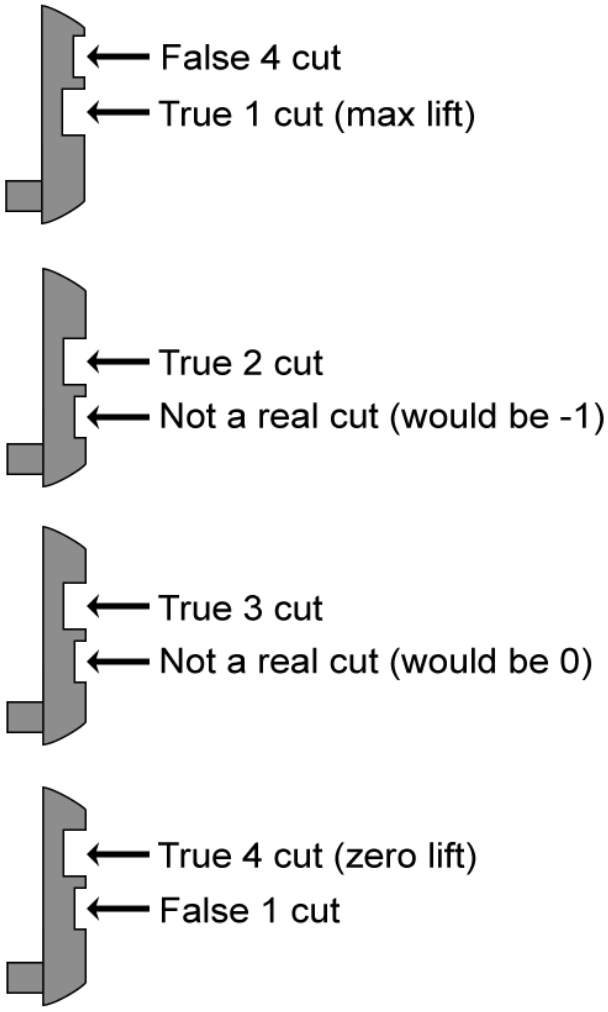
Older false gate design

However, I have never seen a CX5 with these false gates in person so I do not know what it would feel like to attempt to pick them.

Back to the newer false gates: note that they are shallower in depth but also slightly smaller in width. A slider caught in a false gate will feel like it has less freedom to move than a slider in a true gate, even if the slider is not binding. Optimally it should be as difficult as possible to tell true and false gates apart, and therefore the false gates should be identical in every way to the true gates except in depth.

With the exception of the 1-cut slider, all false gates are positioned *below* the true gate. In most picking attacks, the sliders will start at the bottom and then be pushed up until they click when they bind. If there are no 1-cut sliders in the lock, and the picker is careful, then the false gates will never come into play at all.

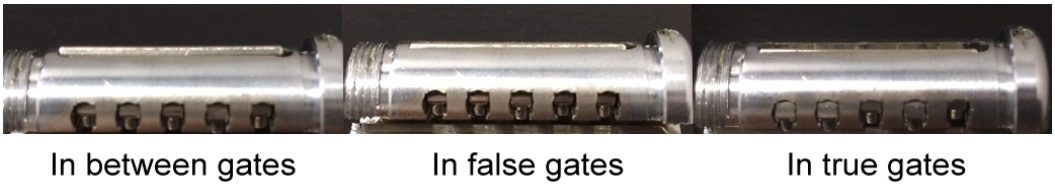
Another flaw in this design is the exact positioning of the false gates. For a 1-cut slider, the false gate is positioned in the same location that a 4-cut would be. The reverse is true for a 4-cut slider. This means the spacing between the false and true gates is equivalent to 3 cuts difference. Therefore, the 2 and 3 cut sliders have no room for any false gates at all. One is cut onto the slider, but the whole range of motion will never actually position it in front of the sidebar. From a manipulation standpoint, they may as well not be cut at all. And as mentioned, the 4-cut has the true gate above the false gate and only oversetting would cause it to engage. A careful picker will only actually have to deal with the false gates on 1-cuts.



All types of slider (to scale, labeled)

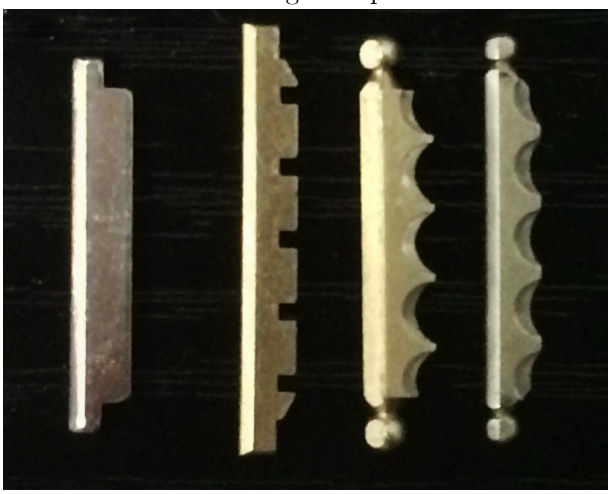
The final flaw with the sliders is that in many cases, but not all the time, the false gates are deep enough to accept the sidebar anyway. 2 and 3-cut sliders obviously cannot do this, but 1 and 4-cuts can.

Sidebar resting positions



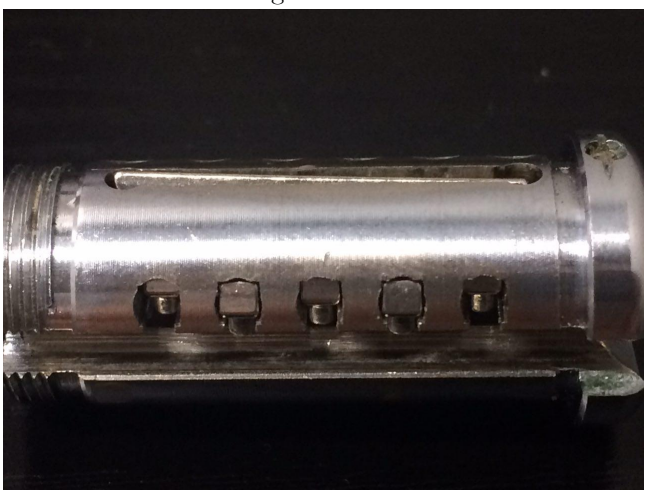
Making this easier is the fact the sidebar has nothing forcing it to remain parallel with the plug, as many other sidebar designs do and this allows the sidebar to rotate a bit and enter the plug at an angle, using some true gates and some false. By using ridges between the side pin chambers, the sidebar has much less room to do this.

Sidebar design comparisons



Shown is the sidebar for the CX5 compared to the sidebars from the Schlage Primus, the ASSA Twin 6000, and the Mul-T-Lock MT5+. Note the ridges between the fences, these help align the sidebar as it enters its slot.

Angled sidebar



Above is a picture of a sidebar where the front three sliders are set to true gates while the rear two are set to false gates. Note the angle the sidebar is allowed to engage the sliders. This is plenty to allow the lock to open with little resistance.

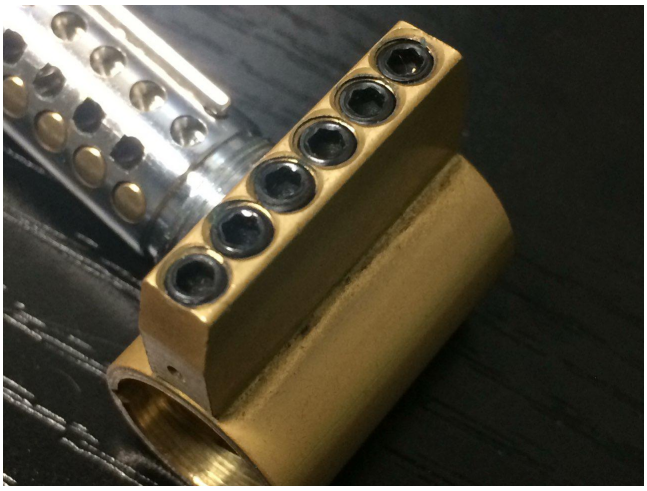
OTHER FEATURES

The CX5 has several other quality-of-life features that really show the amount of thought put into the lock. For instance, a small dimple is drilled onto the front of the housing to indicate which end is the front (the plug can only go in one way):

In addition to the many other features that are intended to reduce the effects of wear on both the key and lock, the dimple on the front of the plug is slightly elongated to make inserting the key easier and to reduce wear against the warding:

This makes inserting the key have very little overall wear against the lock: the dimple on the face effectively guides it into the warding, the pins have very weak springs so as not to produce too much friction, and the sliders are springless entirely and make minimal contact with the chamber walls.

The top of the bible on several formats plugs the chambers with set screws. The LFIC version uses a sliding brass cover plate, however I do not have one of these in my collection. Only the SFIC version uses pressed-in plugs. This makes it very easy to access the pin chambers without the need to disassemble the lock or mess about with the sliders.



Set screws plugging the pin chambers

It is clear to me that many measures were taken in the design of the lock to make the lives of locksmiths servicing them easier. A lot was done to ensure the lock will have a long trouble-free operational lifespan.

MANIPULATION STRATEGY

So far I have discussed several flaws with the designs of both the pin-tumbler portion and the slider-sidebar portion of the lock. In this section I will join them all together and provide a full manipulation guide.

Typically, the pins will bind first and afterward the sliders will bind. This is probably not *always* the case, but it holds true the vast majority of the time.

1. Attempt to overlift the pins. This step may fail if the lock is not vulnerable, but other than the branding on the face there is not much indication of whether this is a possibility from the outside. To execute an overlifting attack, use a pick or other thin tool to press all of the keypins to the very top of the keyway. Apply heavy tension to the cylinder, then slide the tool out. Release tension is a slow, pulsing motion while listening for clicks. The plug will turn partially if the overlifting attack is successful. If you hear a particularly sharp click, this usually means that a driver pin has fallen into the plug and you will have to start over. If the overlifting attack works, skip to step 3.

2. If the overlifting attack fails, the pins will need to be picked traditionally. Using single-pin-picking or otherwise, lift the pins while applying tension such that they all click against the countermilling, then continue lifting to try to bypass it. The countermilling will only fully engage the gin bottles when every pin is either at the shear line or at the countermilling and the plug can turn slightly. The last pin you lift will fully engage with the countermilling, and you may need to partially release tension to get it picked. This is by far the hardest step in picking this lock. In particular it can be difficult to detect when all of the pins have cleared the shear line and in many cases the sidebar can begin to engage before this happens.

3. Once all the pins are picked, the sidebar will begin to butt against the sliders. First, ensure all the sliders are pressed as far to the bottom of the keyway as they will go. Using a short hook or flag tool, slide along the bottom of the sliders, gently lifting each one without lifting the tool (take advantage of the round shape of the fingers). Find a slider that is stiff and push it up

gently until it clicks without releasing tension. If the lock is vulnerable to the false gate exploit, repeating this step will cause the lock to open. If it does not, continue to step #4.

4. If you the lock does not open when all of the sliders are in gates, then the false gates are not deep enough to accept the sidebar. Only 1-cut sliders have false gates that matter (as long as you have not overlifted any sliders) so odds are there are very few sliders with false gates actually engaging, most likely only one or two. It is possible to feel the amount of freedom a slider has and determine the false gate by width, but it is easier and more reliable to probe for sliders that are tightly bound. Once you find one, partially release tension while very gently pushing up on the slider. If you apply too much force, the false gate will pinch the sidebar and seize up the entire sidebar mechanism. Once it starts to move, nudge it up slightly and then reapply tension. Continue to push the slider up until it clicks into a gate. Repeat this enough and the lock will open.

In total, three major design flaws can be exploited that greatly reduce the manipulation resistance of the CX5, which is an otherwise well-designed lock:

- Pinstack overlifting
- False gates accepting sidebar
- False gates not coming into play

As a word of caution, remember that sometimes key pins are too short to actually push driver pins into the bible. If this is the case, picking will very likely destroy a spring and damage the lock.

FINAL THOUGHTS AND RECOMMENDATIONS

Throughout the previous sections I have mentioned several ideas for making the lock more formidable and usable. I have recapped them all below.

- Use pinstack balancing by featuring two or more different heights of driver pin
- Reduce the diameter of the tip of the gin bottles so they better engage with the countermilling
- Use donut-shaped master pins and matching slots for construction keying
- Ensure the diameter of the driver pin is as close as possible to the diameter of the keypin
- Significantly reduce the size of the fence on the sidebar and therefore the true and false gates
- Add material to the spaces between the sliders in the sidebar groove, and cut corresponding slots in the sidebar to ensure it engages with the plug straight
- Place more false gates per slider and some above and below the true gate wherever possible
- Ensure the false gates are not deep enough to accept the sidebar and allow the plug to turn
- Use more than 4 possible cuts per slider (at least 5, possibly 6)
- Support multi-section keys (and possibly produce the lock in more variations of the B/C keyway)
- Support at least 4 sliders in 6 and 7-pin SFIC systems