ISBN: 9798379325701

PREFACE

Locksport is the term given to the hobby of picking locks. This has grown exponentially in recent years due to lockpicking being a fun and challenging puzzle. Safecracking is a form of locksport that is also seeing a rise in popularity. There are many legitimate reasons to learn safecracking. One could be coming from a locksport perspective; wanting to not only challenge their mind with picking keyed locks but manipulating open safe locks as well. One could be a locksmith wanting to expand upon their current skillset. Or one might simply need this information for practical personal purposes such as retrieving a lost combination. There does not need to be a justification for learning this skill. Even if you only wish to learn about the insecurities of a product which is meant to keep your valuables secure and have no desire of ever applying this knowledge yourself.

My biggest hope is that the general public becomes aware of how relaxed lock companies have been with their security and how vulnerable that leaves everyone. This is somewhat known with keyed locks, although still not at a level which I am happy with, but it is largely unknown with mechanical safe locks. The security of these products will not improve on their own. Companies have no incentive to spend money to create a better product if customers are in the dark about how vulnerable these products are. Only widespread knowledge and a public push to improve could cause an improvement in security. As for digital safe locks, they have their own issues which make them inferior to mechanical locks for most applications, despite the glaring flaws which I discuss, although that is outside the scope of this book since I will only be covering the flaws of common mechanical safe locks. But suffice to say that there are enough security holes in the software and hardware that commercially available tools can open them sometimes in seconds.

The knowledge taught within this volume is not meant for use in any illegal manner and I do not condone using this knowledge in such a way. For higher security locks, I don’t give as detailed of information and instead rely on the reader understanding the previous concepts to deter those simply looking to use this knowledge for illegal gain. It is, in my own opinion, borderline criminal to try and keep this information secretive. Criminals have had access to this information for many decades already. Books which are nearly 100 years old that teach on this subject are still relevant due to the lack of innovation in safe lock design. My aim is to bring this knowledge to the honest end user. It pains me to see major governing bodies for locksmiths and safe

technicians trying to hide the insecurities of these products. This aids criminal activity by ensuring the continual purchase of low security products by customers who have no idea how vulnerable they are.

A choice which I have made in this book which differs from the first edition is the inclusion of manipulating “high security” safe locks. I have spent much time debating whether or not this information should be included. I ended up including this information since, while harder to find, is not immune to discovery. If the honest hardworking safe technician has the ability to open these locks, where did that information come from? Someone had to have discovered these techniques at some point. It would be illogical to assume that only law abiding security researchers are able to discover these techniques. Criminals have much to gain and thus massive incentive to discover these techniques as well. Many places also have no such thing as locksmith licenses and anyone in these areas, including criminals, have the ability to portray themselves as law abiding and learn all of this information through legitimate channels.

Contents

Security ratings

This chapter will cover the different security ratings of mechanical safe locks and some terminology that will be covered throughout this book. I will only be covering U.S. ratings as other countries have their own which I am not familiar with. The most common rating for safe locks are UL 768 ratings, with UL standing for Underwriters Laboratory. These go from, in order of least secure to most secure, Group 2, Group 2M, Group 1, and Group 1R. All four of these ratings share the requirement that the lock has at minimum 1 million unique possible combinations.

Group 2: These are the least secure and have very few requirements. This rating allows the combination which opens a lock to have an error of up to 1.25 increments away from the true combination (1.5 if the lock has 4 wheels). Meaning if one of the numbers in the combination is 20, you may be able to dial 18.75 or 21.25 and the lock will still open. This opens a 2.5 increment range thereby drastically reducing the number of practical combinations a lock may have. There are no minimum time requirements against manipulation nor are there any features to thwart against manipulation. These are the standard locks that come with the majority of safes. Almost all of these locks work identically.

Group 2M: This rating is where features to thwart manipulation start to appear. They are supposed to resist manipulation for up to 2 hours, although we will see how these locks fail far from that time. They still for the most part are able to be opened with a 1.25 increment error in dialing. These locks are commonly used on ATMs and burglary rated safes. These locks vary in their design to achieve this rating.

Group 1: This is the highest rating available against manipulation attacks. These are supposed to resist manipulation for up to 20 hours and just like Group 2M we will also see how they massively fail at that. These must be accurate within 1 increment when dialing the combination which leaves a 2 increment gap thereby still drastically reducing the number of practical combinations possible. If a Group 1 lock has a 4 digit combination then it is allowed to have a dialing error of up to 1.25 increments.

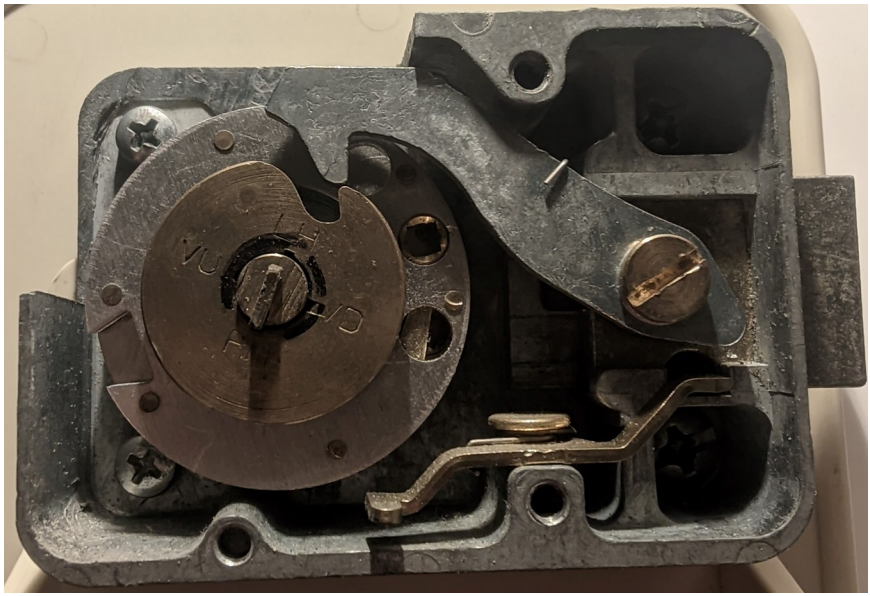
Group 1R: This simply expands upon Group 1 locks with the requirement that they can also resist radiological imaging attacks. This is usually employed through the use of plastic (most often Delrin) parts inside the lock although some may use lead shielding.

I do not know what sort of testing goes on to certify locks in these ratings as many do not even approach the time requirement against manipulation in their respective rating. Pricing of these locks across the different ratings do not drastically increase so I always recommend the highest security lock you are able to get. Sourcing these locks from a locksmith or safe technician may be more expensive and I usually recommend buying one online and paying a qualified professional to install it if you are uncomfortable installing it yourself.

HOW SAFE LOCKS WORK

This will explain how Group 2 safe locks work as Group 1 safe locks follow the same principle and simply add onto it. Group 2 safe locks are almost all identical. The differences lie mostly in small technical details such as how changing the combination works. But the way combinations are entered and the mechanics that happen inside to lock to allow a combination to open a lock are virtually identical.

I will use a Group 2 S&G 6730 to demonstrate the workings of these locks. It is highly recommended that you come back and refer to this often as the terminology for these parts will be used throughout this book.

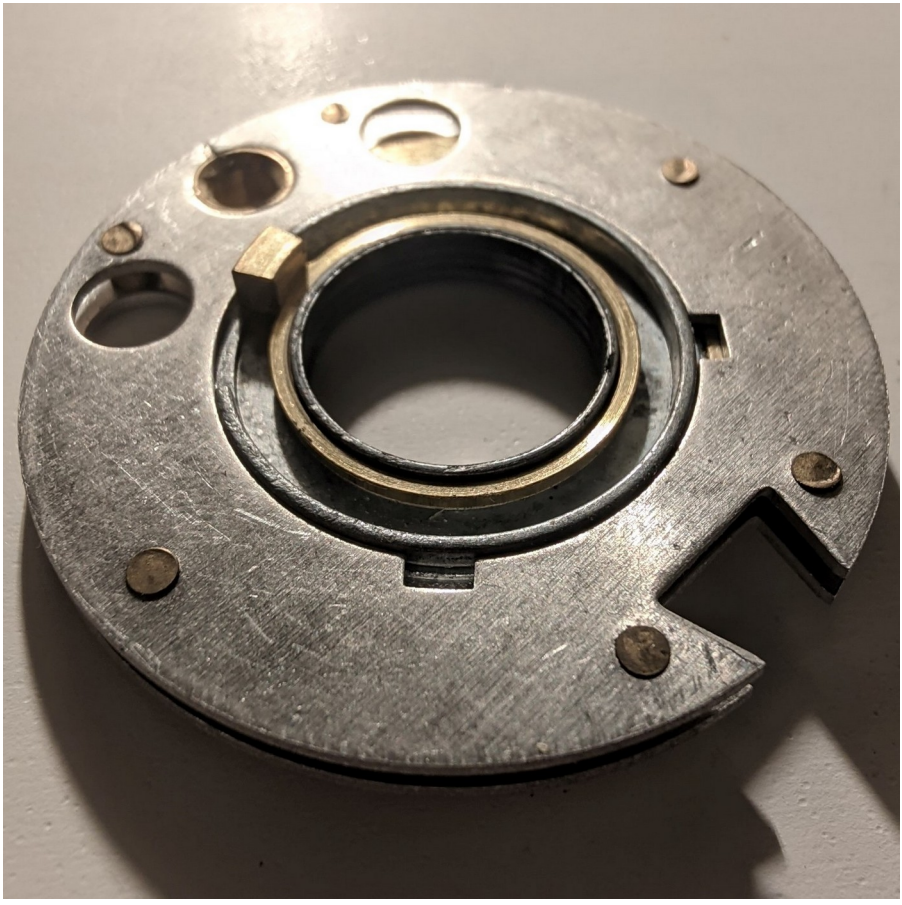


This is the back of an S&G 6741with the back cover removed. The only difference with this specific lock and others of the same make and model is this is a custom cutaway version I made to show the internals while the back cover is on and thus is missing the top left corner of the body. I do not recommend making a cutaway model in this specific fashion though as I do remove part of the lock body which is required for the lock to function properly, specifically to reset the lever assembly when re-locking.

On the left is the dial, face down. The metal threaded rod sticking out the back is called the spindle. It gets threaded through the part on the right called the drive cam and then locked in place by the small “L” shaped piece of metal called the spline key. This makes it so that any rotation of the dial is directly translated to rotation of the drive cam.

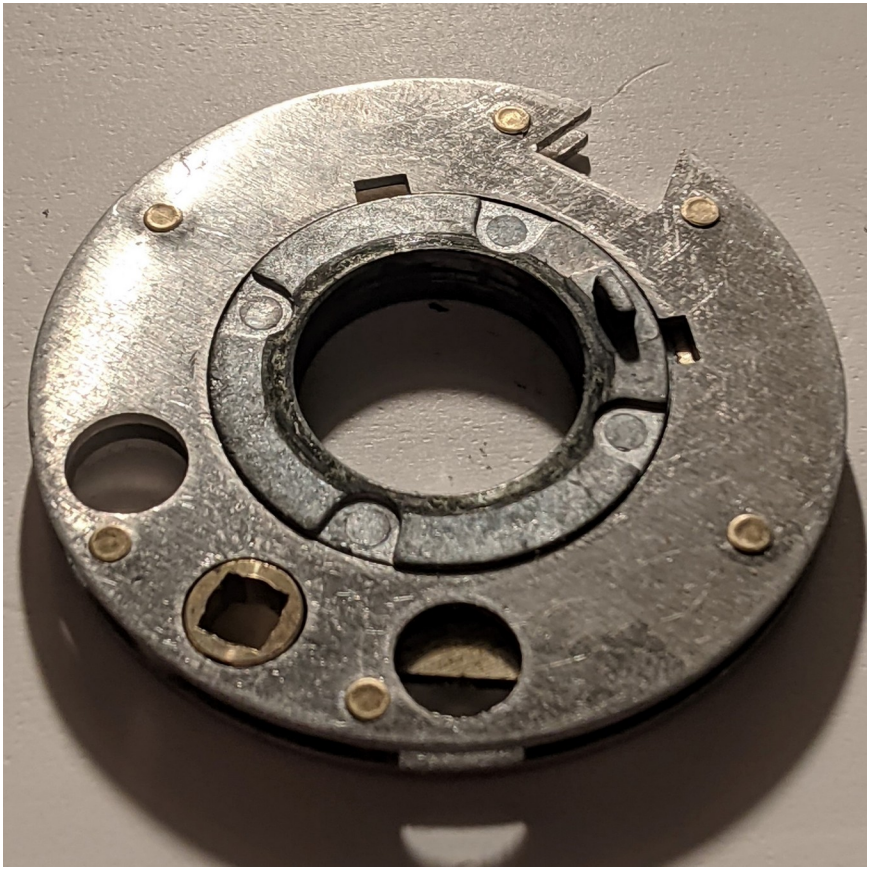
This is the reverse side of the drive cam. Take note of the protrusion on the top right, called a drive pin. The cutout in the drive cam is called the contact area.

This is the lever assembly. On top is the spring which applies constant downwards pressure. On bottom is the screw which holds the lever to the bolt. You can see the bolt in the picture on page 7, it is the protrusion sticking out the right side of the lock body. The middle piece is the lever. It has two main important components, both on the left end. The bar sticking out at a 90 degree angle is called the fence. The protrusion sticking down is called the nose and it rides on the drive cam unless the contact area is underneath the nose. At which point the force from the spring allows it to drop slightly into the contact area. The fence will then hit the wheel pack, keeping the nose from dropping fully into the contact area of the drive cam. This will be further explored more later.



All the wheels are essentially identical so I will cover the parts of them using just one. There is 1 wheel per number in the combination so a 3 number combination lock will have 3 wheels. Each wheel is numbered. From the perspective of the back of the lock, such as on page 7, the 1st wheel will be at the very back. Then the 2nd wheel, and then the 3rd wheel being the visible wheel closest to the back cover just underneath the drive cam. Each wheel also has a cutout in it which is called a gate. The wheels have a center section which is locked in place and can be unlocked and rotated. The location of the gate relative to the inner section corresponds to a number in the combination. I won't cover this in detail as it does not pertain to manipulation.

Like with the drive cam, the wheels have a drive pin on one side and on the other, a movable fly which is the bit of brass sticking up on the top left. You can also see that there is a groove cut into the wheels. The drive pin of the drive cam will ride in the groove of the 3rd wheel and rotate freely around, without moving the 3rd wheel. Once it encounters the movable fly of the 3rd wheel it will interact with it and will “pick up” the 3rd wheel. Meaning that the drive cam will spin with it’s drive pin riding freely in the groove until the drive cam’s drive pin hits the 3rd wheel’s movable fly, at which point the 3rd wheel will start spinning with the drive cam. If the rotation of the drive cam is reversed the 3rd wheel will remain where it is until a full rotation has been made and it hits the 3rd wheel’s movable fly and pick it up in the opposite direction.



This is the back of a wheel. The important part here is the drive pin sticking out on the top right near the center hole; you can see the shadow it casts. This drive pin will ride in the groove of the wheel behind it and interact with the movable fly of that wheel the same way the drive pin of the drive cam and 3rd wheel interact. The next part is the most important in understanding how a safe lock operates.

The drive pin of the drive cam rides in the groove of the 3rd wheel until it hits the movable fly on the front of the 3rd wheel causing the 3rd wheel to be picked up with the drive cam and rotate together.

The drive pin on the back of the 3rd wheel will ride in the groove on the front of the 2nd wheel until it hits the movable fly on the front of the 2nd wheel. Then the 2nd wheel gets picked up and will rotate with both the 3rd wheel and drive cam.

The drive pin on the back of the 2nd wheel will ride in the groove on the front of the 1st wheel until it hits the movable fly of the 1st wheel. Then the 1st wheel gets picked up and thus all wheels and the drive cam will be rotating together as long as the same directional rotation is maintained.

This is by far the most important thing to understand. You will not have any success if you do not understand how the wheels move and interact with each other. I suggest you purchase a safe lock to practice with and view the wheels as you spin the dial to fully understand. You can look online such as on ebay to find locks and lock stands to practice with. The image below shows how the wheels interact with each other, simplified. The black piece is the drive cam, blue is wheel 3, green is wheel 2, and red is wheel 1.

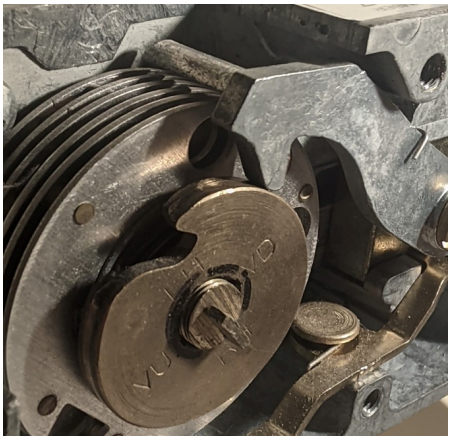
The correct dialing procedure for a combination is as follows:

1. Dial the first number four times to the left.
2. Dial the second number 3 times to the right.
3. Dial the third number 2 times to the left.
4. Turn the dial to the right until it stops moving.

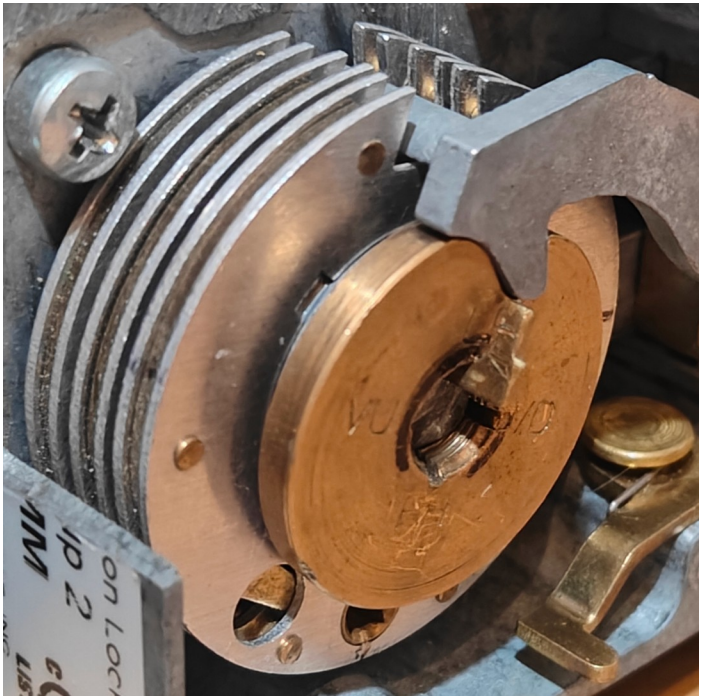
Start out by rotating the dial left (counter clockwise) 4 times to the first number. This means passing the first number 3 times and stopping on the fourth. This is so that no matter the state of the wheel pack, you are guaranteed to pick up the first wheel. A worst case scenario of all wheels previously having been picked up with right (clockwise) rotation means that it takes 1 full rotation to ensure the 3rd wheel gets picked up. A second full rotation will pick up the 2nd wheel and a third full rotation picks up the 1st wheel. That is 3 full rotations to pick up all the wheels hence passing the first number in the combination 3 times. And you still have to set the first wheel so stopping on the fourth time does just that. It does not mean you always need to do 3 full rotations to ensure the 1st wheel gets picked up. It is simply 3 full rotations to guarantee the 1st wheel gets picked up from any random position of the wheels (during manipulation we will know the positions of each wheel and we can utilize this knowledge to avoid spinning the dial an unnecessary amount of times).

Then we reverse rotation and go to the 2nd number 3 times with right rotation (pass it twice, stop on the 3rd). This picks up the 3rd wheel, then picks up the 2nd wheel, then sets the 2nd wheel.

Then rotate left twice to the 3rd number (pass it only once and stop on the second). This will pick up the 3rd wheel and then set the 3rd wheel. Then spin right and the dial will stop moving when unlocked (if entered correctly).




In these two pictures you can see the parts of the lock put back together. The left image shows the nose riding on the drive cam. That causes the fence to be lifted up off the wheel pack. When the contact area is underneath the nose, this allows the fence to drop down onto the wheel pack. The nose drops slightly into the contact area while the fence resting on the wheel pack keeps the nose from dropping down entirely. This is essentially testing if the correct combination has been entered. When the correct combination has been entered, the gates of each wheel will be aligned underneath the fence.



LIST OF MOST COMMON SAFE LOCKS

Group 2

S&G 6730/6741: These two models are virtually identical. The difference is that the 6741 has more room for dialing error which makes manipulation easier. Either of these two models are standard for learning manipulation.

LaGard 3330: The wheels on these locks are slightly oval in shape due to the fact that they are stamped out of a sheet of metal. This means that the shape of each wheel can essentially mask the gate of another wheel. Not recommended for someone who is learning manipulation for the first time.

Diebold 177: Has a drive cam with a symmetrical “U” shaped cutout which means both contact points must be read for accurate manipulation. Slightly better indications from the left contact point.

Big Red Group 2: Same design as the S&G 6700 series but with red wheels.

Group 2M

S&G 6630: Has a roller on the nose to make taking contact point readings more difficult. Also has false gates in the wheels.

La Gard 3332: Listed as Group 2M but seems to have the same design as the Group 1 LaGard 1985. When the contact area is under the nose and the dial is turned, a “tomahawk” like mechanism lifts the nose before contact with the drive cam is made.

La Gard 3390: Similar to the LaGard 3332 but replaces the spring on the “tomahawk” with a slider interacting with the lever.

Group 1

S&G 8500: Uses modifications on the lever to keep it up at all times until the dial is pushed in at the 0 mark at which point the lever gets released and it snaps the fence down onto the wheel pack. If the combination is incorrect, it rises back up partially; far enough that the nose will not make contact with the drive cam and no contact points will be felt. The modified lever is reset by a roller on the drive cam.

S&G 8400: Has a more complex drive cam with a shutter, activated by a device on the front of the dial, that prevents the nose from touching the drive cam.

S&G 2937: The same as an 8500 series just beefed up to withstand physical brute force attacks better.

La Gard 1985: Similar to the La Gard 3332 but with a better attenuated spring.

Mosler 302/402: Has a split drive cam with serrations that catch and spring past the contact point. Also has 16 sided wheels instead of circular wheels. The 302/402 just refers to having either 3 or 4 wheels, respectively.

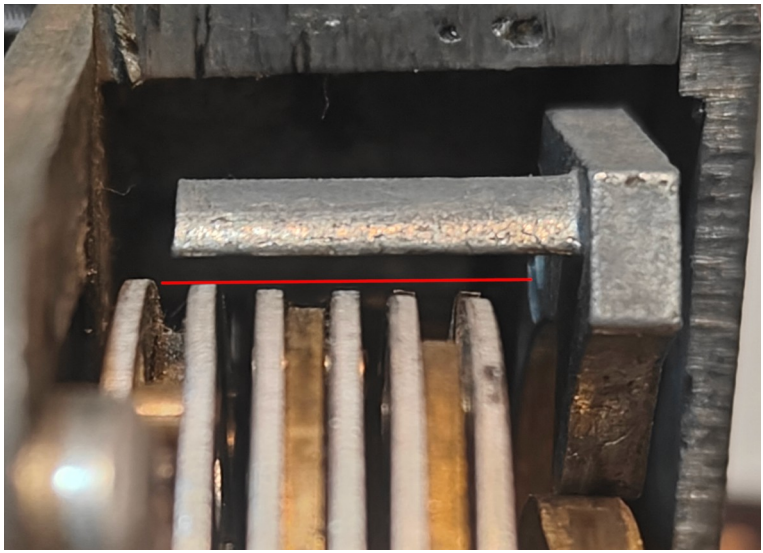
Vulnerability

The vulnerability of safe locks is the fact that we are able to get feedback from the lock, and most importantly, that feedback changes depending on the state of the internals. In this case, the feedback we receive is the contact point; the nose hitting the drive cam when coming out of the contact area. As we spin the dial, we can feel the nose hitting the drive cam as a bit of resistance in the dial. Note that we must spin from inside out so spinning the dial left from the front of the safe we will hit the sloped side. This is called the right contact point as from the front of the lock it is on the right. And we spin right to feel the left contact point.

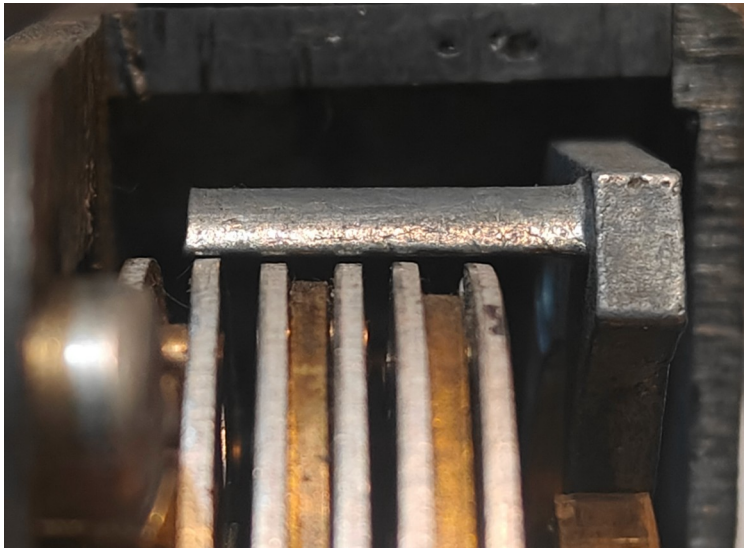
Looking at how the contact area is shaped, we can see that one side is sloped significantly. This means that the lower into the contact area we go, the less distance there is between the two walls. It's wider at the top and narrower at the bottom. Now imagine the nose in the contact area but at the top. If we turn the dial and feel the two contact points they should be relatively far apart. But if the nose is low in the contact area, the two contact points will be felt closer together. The numbers on the dial when we feel the contact points will change.

The distance the nose drops into the contact area actually changes depending on the position of each wheel. Obviously if all gates are aligned under the fence then the nose will drop completely into the contact area. But even without this, the position of each wheel determines how far down into the contact area the nose goes.

You must understand how a lock works and the why behind how the lock is vulnerable to be successful at manipulation. Without this you will find it incredibly difficult to get very far in this hobby. The material can be frustrating to mentally grasp in the beginning but it is something that once you know and understand it will become second nature.



The above image shows that each wheel is differently sized. You can see that the 1st wheel (leftmost wheel) sits higher than the other two. This is because it's impossible to make all wheels exactly the same size or even perfectly circular. This means that there will always be a wheel that is larger or simply has a bump on it that lets it sit higher under the fence than the other wheels. Below you can see the effect of this, the fence only rests on the largest wheel.



If the fence only rests on the largest wheel but then we rotate that wheel, and only that wheel, so that it's gate is under the fence then fence will drop down slightly to rest on the next largest wheel. This means the nose too will drop and rest lower in the contact area. And with that, we can feel the contact points closer together which tells us one of the wheels has it's gate under the fence. We can use this information to figure out an attack that lets us know one, what number on the dial causes the fence to drop and two, which wheel causes the fence to drop. This gives us the correct number for that wheel. Keep in mind that it's not always the largest wheel that the fence will rest on first, another wheel could have a bump that extends further.

It is also common to only take readings of the right contact point as it is more sloped and will give greater indication of change than the left. However, when starting out it is always a good idea to take readings of both contact points for extra corroboration and practice in feeling the contact point.

Group 2 Manipulation

So we know the following:

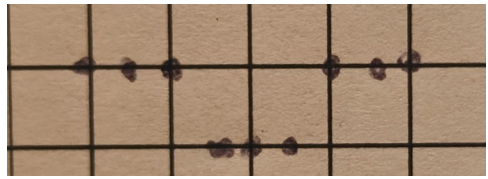
- The wheels are all different shapes and sizes.
- Thus the fence will only rest on 1 wheel at a time.
- If the largest wheel has it's gate under the fence, the contact points will be closer together than if it does not have it's gate under the fence.

We can now put what we know together to devise a plan of attack. Let's say every time we take contact point readings, the third wheel is advanced 2 increments further. Then at some point, the gate will be under the fence and we should see a drop in the right contact point and an increase in the left. To initially find the contact point, simply spin all wheels to 0 so that we know where they are and we don't accidentally mistake the feeling of picking up a wheel for the contact point. Then spin the other way until you feel the contact points. An important note is that sometimes the contact point will have a "bump" and it will feel as if there are two of the same contact points. So if feeling the right contact point we might feel a slight resistance and then another just after it. This can be due to either debris or wear and tear on the parts. We simply want to make sure we are consistent and always feel the first point.

We can actually discard the left contact point as the right contact point gives much better indications due to the sloped edge of the drive cam. If we only have 1 wheel changing position between contact point readings, we then know that when we feel a drop in the right contact point, the number we just set that wheel at is it's number in the combination. This method is called wheel isolation as we only have 1 wheel changing positions each time we take a contact point reading. We'll use this method and refine it in order to grab all the numbers in the combination in an efficient and reliable manner. Here's some additional information that will help:

- The largest wheel is not always the largest wheel. Other wheels may have bumps that sticks out "shadowing" that wheel (the bump being the highest point of all three wheels for that moment).
- The drive cam usually rests on wheel 3 first and if not, then usually wheel 2. This is due to the spring applying pressure on the lever, causing the fence to tilt.

- If taking contact point readings across an entire gate, it will present itself as a drop in the right contact point for a few increments, then a rise back up, mimicking the shape of a gate as seen here.



With the 3rd wheel most commonly being the one the fence rests on we should isolate wheel 3 first otherwise the 3rd wheel will shadow the first two. But if we just leave wheels 1 and 2 at random locations, they may shadow the 3rd wheel if they happen to protrude out. That risk is not too great but there is a method which can vastly reduce it in a short amount of time. If we pick up all the wheels and take contact point readings every 10 increments, we can determine an approximate “common low point” across the wheel pack. So for instance spinning right 3 times to ensure all wheels are picked up and leaving them on 0, then turn left to the right contact point and take a contact point reading. Then turn right to 0 picking the wheels all back up and continuing to 90. Rinse and repeat until you have 10 contact point readings. We take our lowest reading and we leave our first 2 wheels there. So let’s say our contact point reading at 30 was the lowest reading. We want to leave the first two wheels at 30 to help ensure they don’t shadow wheel 3 and then change the position of wheel 3 by 2 increments every time we take contact point readings.

We also advance a wheel by 2 increments each time due to the fact that the width of the gate is wider than the width of the fence. There is approximately a range of 3-4 numbers that each wheel can be dialed with and still open the lock. So we go by 2 increments instead of 1 to speed things up without risking us missing a gate being present under the fence. We usually see a drop in the right contact point of about 1/4 increments for 2 readings in a row as a gate signature, although a drop for a single reading can happen.

Starting out, we want to keep track of our contact point readings as we go (as you get more experience you won’t need to graph your results) so I’ve included sample graph paper on the last page. You can easily just make your own with normal graph paper or copy it to print out. There is room to include both left and right contact point readings if you wish to take both or simply space for 2 right contact point reading graphs. Space is also provided below for any notes you may have for yourself during the process. The middle of the black boxes will be the closest whole number to the contact point with the boxes next to it being one

higher and one lower. The numbers along the top indicate where we've left our wheel. Then we simply place a mark at the corresponding intersection. Each horizontal graph line (when the paper is viewed in landscape orientation) is 1/4 of an increment. We ideally want to read the dial in 1/8 of an increment so we just place our mark in the middle of two lines to get 1/8ths of an increment.

Important tips:

- It is important that reading the contact point is as consistent as possible. You must look at the lock straight on at the same angle each time and feel the contact point with the same amount of force each time.
- You must read the number on the dial as precisely and consistently as possible. Using increments of 1/8 is relatively easy as you can just divide the space between increments by 2. You must be consistent as well. Seeing 3/8ths of an increment must always be the same and not to be confused with 2/8ths or 4/8ths.
- If the dial is hard to read, you can print out a vernier scale and tape it to the dial/dial ring since the markings that come on the dial/dial ring are wide and imprecise.

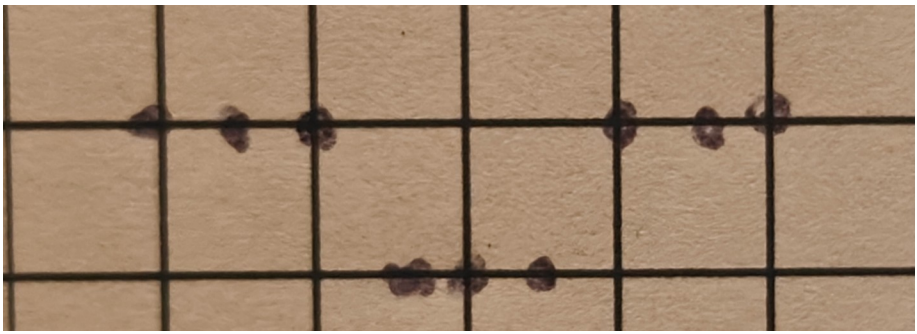
Isolating wheel 3

When we dial a combination into a lock we always dial the 1st and 3rd number with left rotation and the 2nd number with right rotation. An important note is that dialing a number with a different rotation will change where it actually is. This is due to the width of the drive/fly pins. So if we're isolating wheel 3, we want to always turn wheel 3 with a left rotation when setting it on a number. This means when we set the first 2 wheels to the common low point (the lowest of the 10 readings we start with) we should do so with right rotation. If we do it with left rotation, we can't rotate left anymore as that will just move the first 2 wheels out of place. This is why I always take those 10 initial readings with right rotation. You might've noticed that for wheel two that means we have to set wheel 1 (wheel 3 should be on it's found number if we're isolating wheel 2) on the low point with left rotation even though we found the low point with a right rotation. That's ok as the difference shouldn't be large enough to cause any significant effect. Finding the low point with right rotation just allows a faster start to isolating wheel 3. So we're going to assume we found a common low point at 30 and the right contact point is at 80. We will start our manipulation 2 numbers higher than the common low point so that we can make a full rotation without disturbing wheel 2. This will be our course of action:

1. Park all the wheels at 30 with right rotation
2. Turn left 1 full rotation to pick up wheel 3 and then keep going left to 32
3. Turn right to the contact area and take our right contact point reading
4. Turn left to where we left wheel 3 and then advanced it by 2
5. Repeat steps 3-4 until we get back to 30 (make sure to take a contact point reading at 30)

As you can see, we don't need to redial each wheel. Since we're isolating wheel 3, and wheel 3 picks up first, we only need to move wheel 3 each time. Now we can look at our graph and look for a 1/4 increment drop that lasts for 2 readings before rising back up. Because we're taking readings 2 increments at a time, that gate signature might not be perfectly centered. So we want to go back and amplify that area. Which means to take readings through that area again but every increment. Starting with the number we initially skipped over. So if the gate signature was at 28 and 30, we start at 27 and end at 31 since we already took readings at 26 and 32. Then we choose the center as our number for wheel 3. We should be precise here as well so if the center is

between two increments such as 28.5, then we put down 28.5 as wheel 3.



Example gate signature after amplicifation

If you can’t identify a gate signature then simply choose the lowest contact point reading to be the “correct” number for wheel 3. It may be that wheel 2 or 1 reads first so we need to make sure wheel 3 is as out of the way as possible and we do this by selecting the lowest point on wheel 3 to leave it at for future wheel isolations. It’s common that there will be multiple readings that are all the lowest contact point reading, i.e. readings for 54-68 were all at the lowest. In this case you can choose any of them for your lowest reading.

Isolating wheel 2

Isolating wheel 2 is similar to wheel 1 but rotations are reversed and we have to worry about parking wheel 3 at it's number we found in the previous step before taking contact point readings. Also, we will be parking our wheels on the common point with left rotation this time so if you wish you may retake your common low point readings but with left rotation instead of right to get a new common low point (returning wheel 3 to it's found number each time).

We dial wheel 1 to the common low point with left rotation, wheel 2 to where we want to start manipulating (I start 2 increments below wheel 1 so we can get a whole rotation without disturbing wheel 1), and wheel 3 to it's found number. So let's say we found the gate on wheel 3 to be 57. We would then dial 30-28-57 then take contact point readings. Now to move wheel 2, we only have to turn right until we reach where wheel 3 was, 57, then turn right to where wheel 2 was, 28. Then turn two increments further to 26. Rotate left 1 rotation to pick up wheel 3 and continue left to 57. Then turn right to the contact area to take a contact point reading and repeat. In a list:

1. Put wheel 1 on it's low point, wheel 2 two increments below that, and wheel 3 on it's gate/low point.
2. Take contact point readings.
3. Turn right to wheel 3, continue right to pick up wheel 2, then continue for 2 more increments.
4. Turn left 1 rotation to pick up wheel 3 and continue left to return it to it's gate/low point.
5. Repeat steps 2-4.

As with wheel 3, we look for a gate signature and amplify it by taking contact point readings every increment through there and choose the center as our number for wheel 2. Or in the absence of a gate signature then we simply choose the lowest reading. We'll choose 88 as our example gate for wheel 2.

Isolating wheel 1

Wheel 1 is the worst wheel to isolate. Hopefully you found good gate signatures for wheels 2 and 3 because if so, you can just dial for example, 0-88-57, 2-88-57, 4-88-57, etc until it opens. Either way, it's still not a bad idea to graph wheel 1 in case you falsely assessed some readings as a gate signature. That way we can still have at least a low point if not a gate for wheel 1.

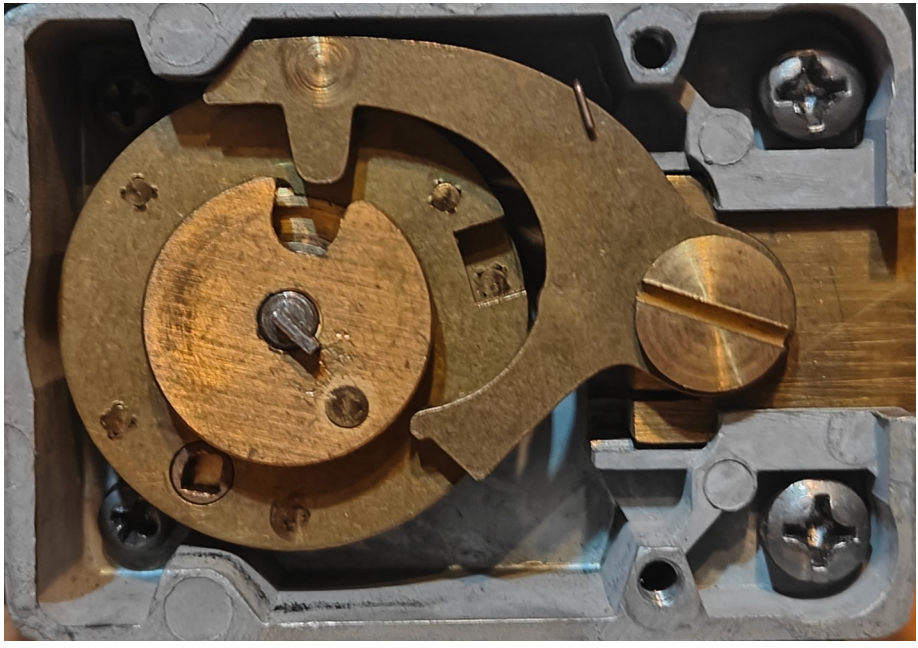
With wheel 1 you are essentially just dialing a full combination each time as you have to pick up the other wheels to move wheel 1 and reset them after advancing wheel 1. But we can be smart about this. If we start at 0 and dial 0-88-57 then take our contact point reading, we don't have to spin the dial 4 times to the left as we normally do when dialing a combination because we know where the wheels are. We just turn left to 57, left only 29 increments more to 88, and that's already wheels 2 and 3 picked up. So we can just turn to 2 from there and reset wheels 2 and 3.

If the lock doesn't open, that's ok. We just select either the gate signature if there is one, or the lowest point and that's our number for wheel 1. Then restart the wheel isolation process with wheel 3 but instead of using the common low point of 30 in our example, we use our found gates/low points for wheels 1 and 2. So for example if the lock doesn't open and we found 12 as our lowest point on wheel 1 then we would re-isolate wheel 3 with wheel 1 parked at 12, wheel 2 parked at 88, and then start isolating wheel 3 at 90.

This successive finding of low points helps to unmask the other wheels so now we should have a really high chance of finding the gate on wheel 3 the second time around. Sometimes you may have to do a few isolations for each wheel. If the wheels happen to read in the order of 1, 2, then 3, that would mean 3 isolations per wheel.

Exceptions

Some locks are a little different and require different handling. For example, Diebold locks have a U shaped drive cam so the right contact is not more sloped and does not give better readings. The left contact point actually gives better readings as the top of the contact point is slightly more sloped than the right. But generally we want to take both contact point readings and look for a decrease in the width between the two as even the left contact point is not always enough to give good indications of a gate.



Diebold 177-23

A really big challenge for people starting out are LaGard locks, specifically the 3330. The wheels are more oval shaped and will almost always shadow each other so multiple isolations of each wheel will be necessary. Some techniques help save time though. Knowing the wheels are more oval shaped, we can take readings every 5 increments with all wheels to start out with. We should see 3 peaks, or just choose the 3 highest contact point readings we find. Keep 2 wheels at the lowest point you found during those 20 readings and isolate each wheel through each peak to find which peak belongs to which wheel. Then we can do our real wheel isolations with each wheel at 90 degrees (25 increments) off their peak to get the low side of the oval. For

example, lets say we see 3 high points at 25, 36, and 81 with our lowest contact point reading at 55. We park wheels 1 and 2 at 55 and take contact point readings for wheel 3 at 25, 36, and 81. The highest contact point reading means that peak belongs to wheel 3. So we'll say that when wheel 3 was at 25 the contact point was the highest. With wheel 1 and 3 parked at 55 and wheel 2 being isolated at 36 and 81, let's say we found 81 to be higher. So we start our wheel 3 isolation with wheel 1 at 36 + 25 = 61 and wheel 2 at 81 + 25 = 6 (106 but minus 100).

La Gard wheels also have a vulnerability due to how the fact that they are stamped from a sheet of metal. Directly opposite of the gate on each wheel will be a bump. This can be detected through isolating each wheel. If a single significant increase and then decrease in the contact point is detected, it can be fairly certain that the gate is exactly 50 numbers away. Although wheel shadowing can obscure this bump.

Alternative Manipulation Method

An older method of manipulation is called “all wheels left/right” or AWL/AWR. Instead of starting by moving only one wheel at a time you instead move all wheels at the same time. Because wheel 3 generally reads first and is set in the combination with a left rotation as well as wheel 1 being set with a left rotation, you generally want to start with AWL for a higher chance of finding a number in the combination with the already correct rotation. Since all wheels move together, you can start at any number and just take readings every 2 increments all the way around the dial.

The issue with this is that there can be bumps on each wheel shadowing the gates on the other wheels. It also means that if you do find a gate signature then you don’t immediately know which wheel it belongs to. That’s where high/low testing comes in. To do high/low testing you run 2 sets of tests. For the high test you put 1 wheel 10 numbers higher than the gate and the other 2 wheels on the gate and read both contact points to find the width. Repeat for each wheel, for example if you find a gate at 25 you will dial 35-25-25, then 25-35-25, then 25-25-35 measuring the width of the contact area after each. If you have already found a number for a wheel, you just substitute it in during this process. With one wheel being wrong, we can expect a wider contact area when the correct wheel is on the incorrect number. Therefore if we found the widest contact area when wheel 3 was on the wrong number then that indicates our gate belongs to wheel 3. We add on to this by performing it again but using 10 numbers lower to be more sure.

If, for example, wheel 3 indicates a gate first here then you would spin wheels 1 and 2 with right rotation together, resetting wheel 3 each time after advancing them. If wheel 2 reads first then you will most likely want to spin wheels 1 and 3 with left rotation again. Even though wheel 2 is set in the combination with a right rotation but we found it with a left rotation we want to keep setting it with left rotation. In this case that would mean all 3 wheels need to be set with left rotation. This isn’t actually an issue as after setting wheel 1 with left rotation, we simply spin right and pick up wheel 2 and go past where it needs to be. By about 5 increments or so. Then turn left and pick it up again and leave it where it needs to be.

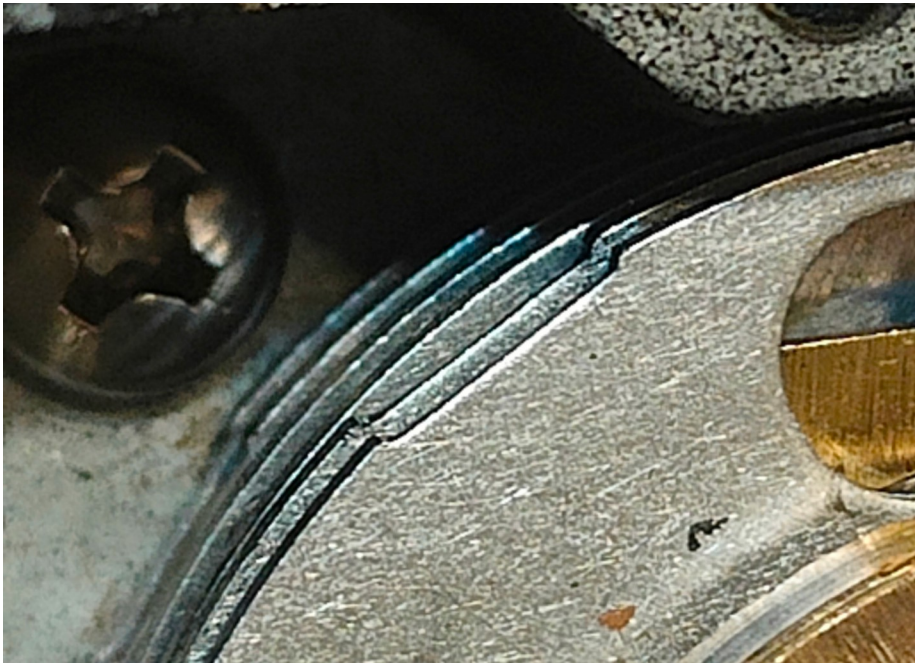
This method can be combined with wheel isolation as well. You can replace the high/low method with wheel isolation by isolating each wheel through the gate signature. You can also start with AWL and if no gate is found, you have a graph to find the common low point to start from for wheel isolation. There is no one right way to do things, if you understand the way different methods of manipulation work then you can combine or change them as you see fit. There will be times I start with wheel isolation and if wheel 1 or 3 indicate first then I will move the other two wheels to the right together instead of continuing with isolating.

Group 2M

S&G 6600 series

The differences between the different models in this series is how many wheels and whether the nose has a roller. They all contain false gates. On the models with a roller, that will look like the image below.

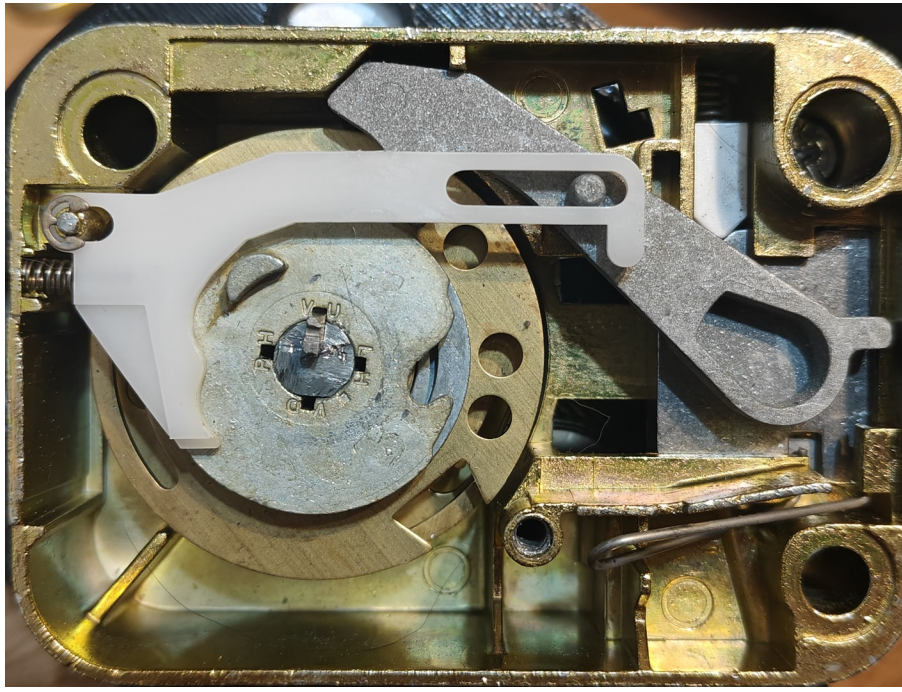
This is a non-concentric roller meaning it spins freely and is more oval on purpose. This is so that if you were to take multiple contact point readings in a row, without moving any wheels in between each, then you will get multiple different results due to the roller spinning each time you take a reading. You can sometimes identify this security feature from the outside as the roller will rattle while spinning on the drive cam. To get around the roller, aggressively tap the contact point a few times before you take a reading and take the lowest or highest of multiple readings as your contact point. You want to make sure you are getting the lowest/highest point possible each time for consistency.



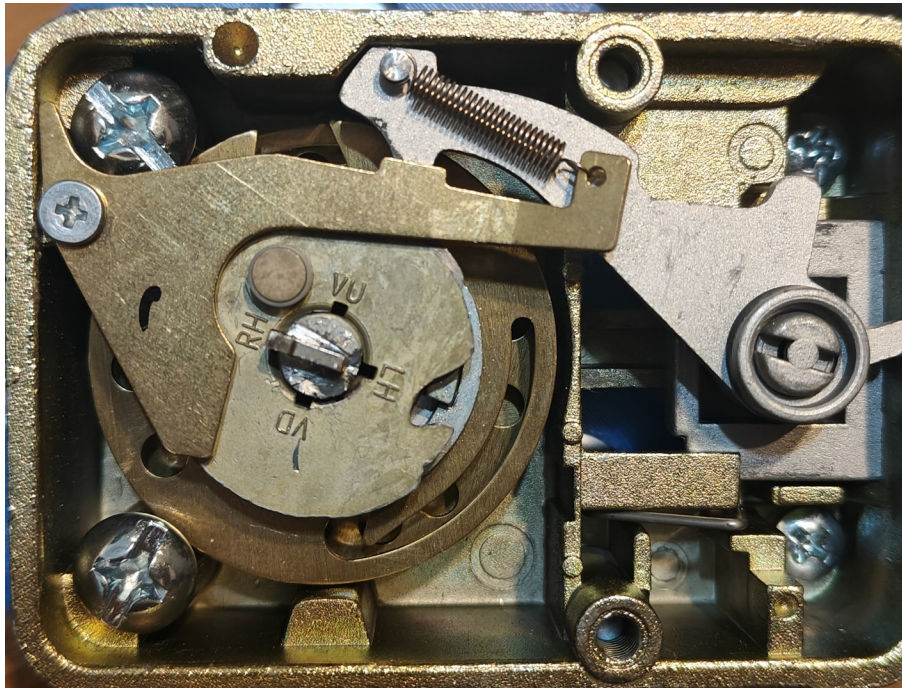
False gates are present in all models and look like very shallow gates on the wheels. They are deep enough that it will look the same on a graph as a true gate. I employ a wheel isolation technique and assume the first gate I find is the true gate, whether it is or not. Then after finding 1 true/false gate per wheel I isolate each wheel again and find the deepest gate signature as my true gate for that wheel.

La Gard 3332/3390

These both operate on the same principle just using slightly differently shaped parts. These both have a Fence Lever Control Device, FLCD, which lowers the fence onto the wheel pack when the nose is over the contact area. If the combination is entered then the lever and nose will get pulled all the way down. It starts pulling the lever down just after it passes first contact point and lets it back up just before reaching the second contact point so you are unable to ever make contact with the nose and drive cam unless the combination has already been entered.



La Gard 3390

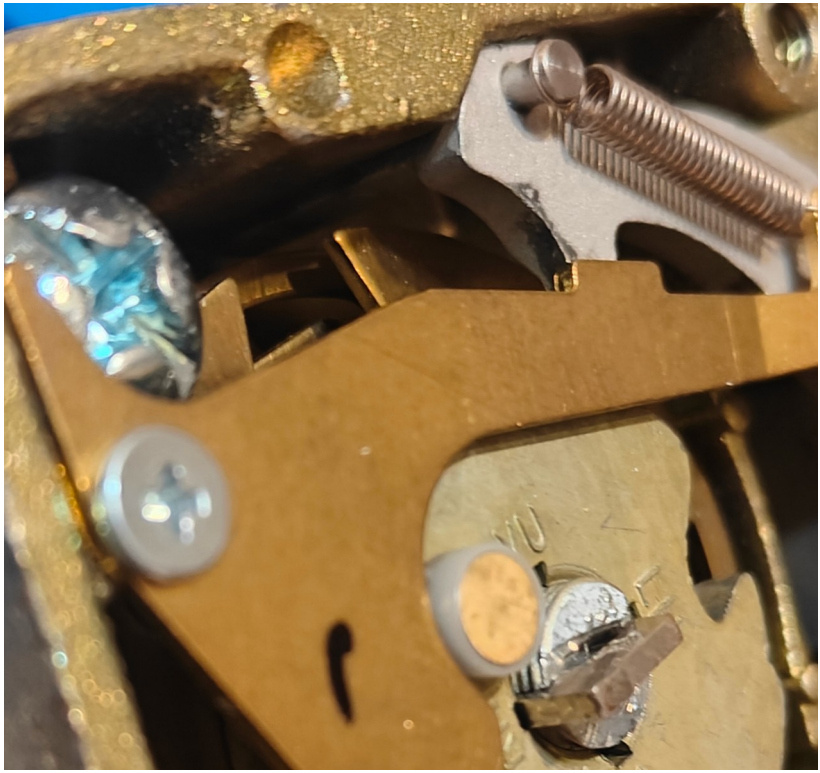


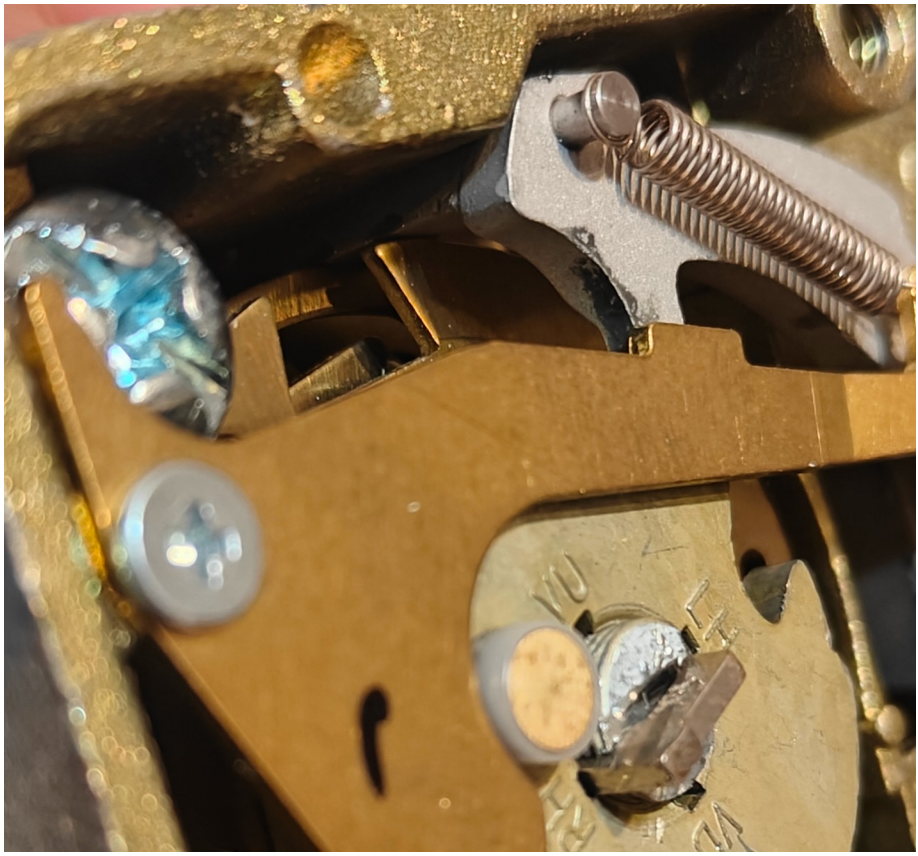
La Gard 3332

The way these locks feel when spinning the dial is like two strong, bouncy contact points that are felt from the outside in. Unlike normal contact points which are felt from turning within the contact area to outside of it, these are felt turning into the contact area from outside of it. They also usually offer more resistance. Along with this there is a constant rotational force exerted on the drive came while in the contact area so the dial will want to bounce back when turning through it.

In this case, our contact points are not the initial position we find resistance. That is the feeling of the FLCD spring being engaged. We want to continue turning until it brings the fence down onto the wheel pack. At this point the wheels will stop the lever from going lower and thus pulling slightly more on the spring. It is very important to practice while looking at the back of the lock to visually see when the fence hits the wheels and correlate it with the feeling of the dial. Because the two FLCDs in these locks are differently shaped, I turn left to read the left contact point (since we approach from outside we turn left to feel the left contact point) on the 3332 and right to feel the right contact point on the 3390.

In the picture below you can see the drive cam has a protruding pin that interacts with the FLCD. Here that pin has just contacted the FLCD and you will feel some resistance through the dial but the fence is still in the up position.





In the above image the dial has been turned more and has engaged the FLCD which pulls the fence onto the wheel pack. This creates extra resistance in the dial and this is the contact point, when the fence hits the wheel pack.

For the 3390, I find it to rattle and make more sound upon initially engaging the FLCD. This might be due to it's design as it's spring is not always under the same tension as the 3332. The 3390 also has a very light initial resistance upon engaging the FLCD and a much more noticeable difference when the fence hits the wheel pack. The 3332 has a very noticeable difference in resistance when engaging the FLCD and a smaller difference when the fence hits the wheel pack. It simply takes some more practice to feel accurately.

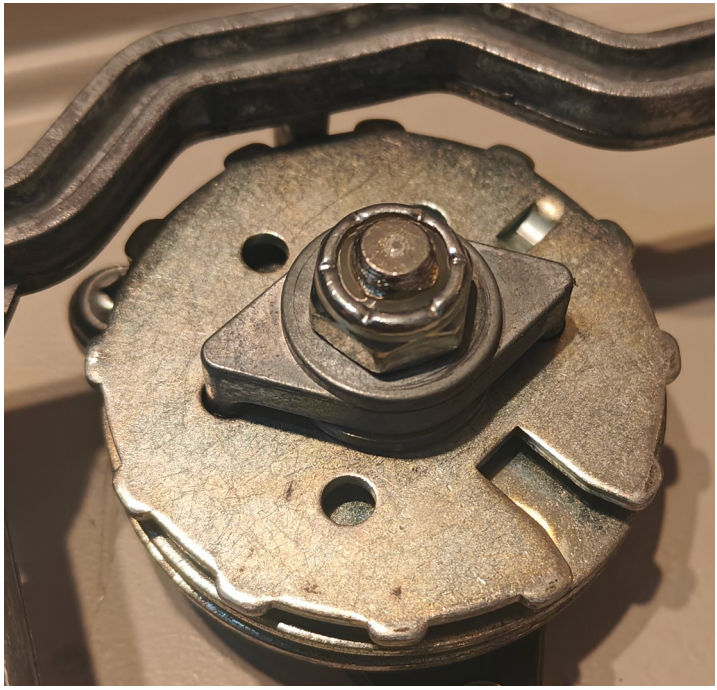
Direct Entry/Star Floor Safes

Before going into Group 1 manipulation techniques, I want to cover some edge cases. There are some locks known as direct entry where there is no spring loaded lever. The fence is attached to the handle and turning the handle pushes the fence into the wheelpack. These are generally lower security locks and found on cheaper safes such as Sentry safes or smaller gun safes. There is also a type of floor safes branded with the name Star that is similar to Group 2 but there will be no contact points felt. This is because the dial actually pushes in at 0 and the contact point is how far the dial is able to move in.

Direct Entry

Direct entry locks usually follow a different set of rules for how the combination is dialed. They usually have one less rotation for each wheel and the direction can be reversed. This is because there is actually no drive cam. The 3rd wheel is directly connected to the dial and acts as a pseudo drive cam. So you would dial the first number 3x, the second number 2x, and the third number you simply go to it once and stop the first time you reach it and leave it there. At this point instead of turning the dial to unlock the safe, you turn the handle instead. This will push the fence into the lock. If all gates are aligned, this allows the handle to turn all the way and retract the bolts, otherwise the handle will stop early because the fence will hit the wheel pack.

This has an obvious disadvantage that you can turn the handle while spinning the dial and just feel when the gates scrape by the fence. For this reason almost all of these locks have false gates. The false can be either on only the 3rd wheel or all wheels. This makes it so that when you turn the handle and push the fence into the wheelpack, the dial will lock up from the fence sitting in a false/true gate on wheel 3. This is the best way to tell if a lock is a direct entry. There will also be no conventional contact points to feel for. The contact point in this case is actually how far the handle is able to turn.



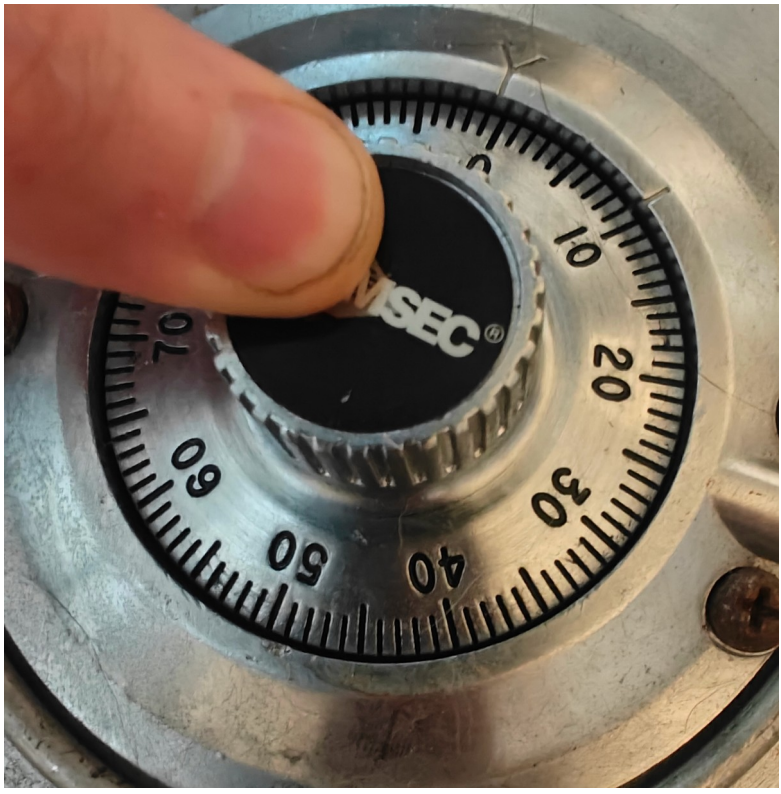
Above is a direct entry lock with the wrong combination entered and handle turned, pressing the fence into the wheelpack. You can see how the false gates on wheel 3 would keep the dial from turning (since it's connected directly to the 3rd wheel). Below is the same lock with the correct combination and the handle turned to lower the fence into the wheelpack.

To measure how far the handle can turn, and thus obtain a contact point, we can simply tape a laser pointer to the handle and have it shine some distance away onto a flat surface. The more the handle can turn, the more the laser dot will move across the surface. And the further away the dot shines, the greater amplification of this movement that you get. The handle must also always be turned with a consistent amount of force each time as materials have bend and using a different amount of force to turn the handle will vary how much the laser moves. I prefer to tape paper to a wall roughly 10ft away and make markings to show the distance the laser moves, with this distance being the contact point. The more the laser moves, the deeper into the wheel pack the fence gets.

Star Floor Safe

Some round door floor safes also have no conventional contact point to be felt either. These are known as Star floor safes but may be branded by a 3rd party as well. Below is an Amsec branded one.

These can be identified through the fact that the dial will press in at 0 as shown below.



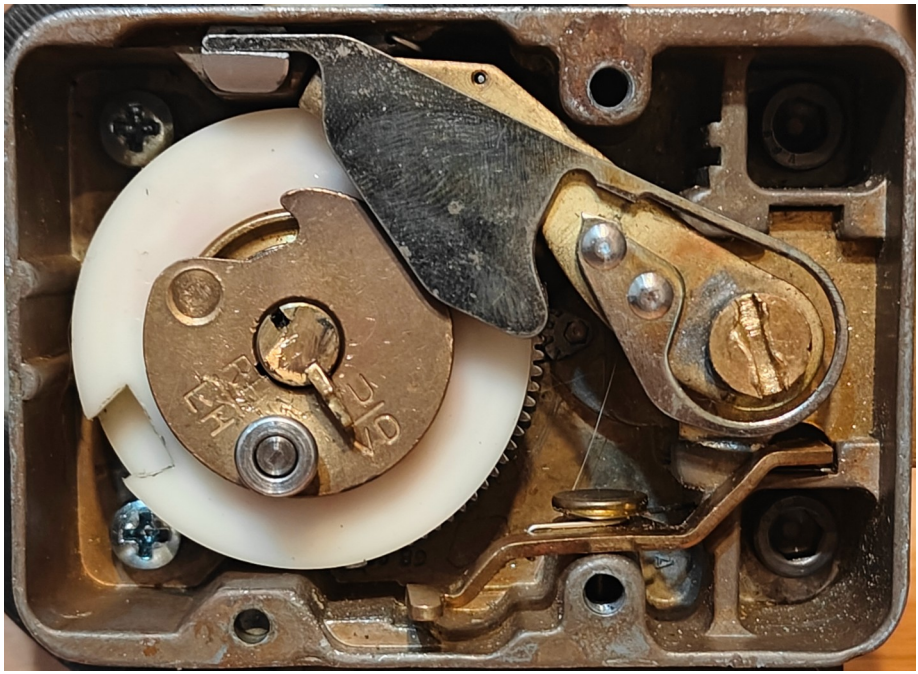
The dial of these safes are also removable as shown below and is another way to tell that the lock is this type.

These locks can still be manipulated with the same techniques as Group 2 locks but the contact point is how far the dial is able to depress. To measure this, one should use a depth gauge with decent accuracy and reliability. This must be mounted securely on the front of the safe and zeroed at the top of the dial. Instead of turning to feel a contact point at a location you instead will turn to 0 and push in on the dial to get a reading of how far the dial is able to travel.

Group 1

S&G 8500 series

These are probably the most popular Group 1 locks in use in America. They work very similarly to their Group 2 counterpart, the 6700 series. The only difference in the operation of the lock is after dialing the combination, the dial is rotated right to 0 and pushed in before rotating right again to retract the bolt.



The wheels on this lock are plastic making it a Group 1R lock. The two main things to pay attention to though is the silver attachment on the lever and the silver protrusion on the drive cam. The addition to the lever holds the fence and nose up so that no contact points can be felt. When the dial is turned to 0 this lines up the middle of the contact area under the nose. After pushing the dial in, the drive cam will hit the lever assembly causing it to drop down. If the combination is not entered then the fence will hit the wheels and bounce back up so that turning the dial doesn't produce any contact points. If the combination has been entered then the fence will fall into the gates and the nose into the drive cam allowing the bolt to be retracted. The protrusion on the drive cam pushes up and resets the lever assembly if the wrong combination has been entered.

The vulnerability with this design is the fact that whenever the dial is turned to 0 and pushed in, the force of the fence striking the wheels cause them to rotate. This generally affects the 3rd wheel first as it's usually the first wheel the fence touches. The rotation is also always in the same direction, left when looking from the back and right when looking from the front. This means that the dial can be pushed in at 0, rotated to reset the lever assembly, and repeated until the 3rd wheel has rotated enough that it's gate is aligned under the fence. Once this happens it will stop rotating by itself as the fence won't strike it anymore. As this point the next wheel to make contact with the fence will start to rotate. In this way the lock essentially manipulates itself.

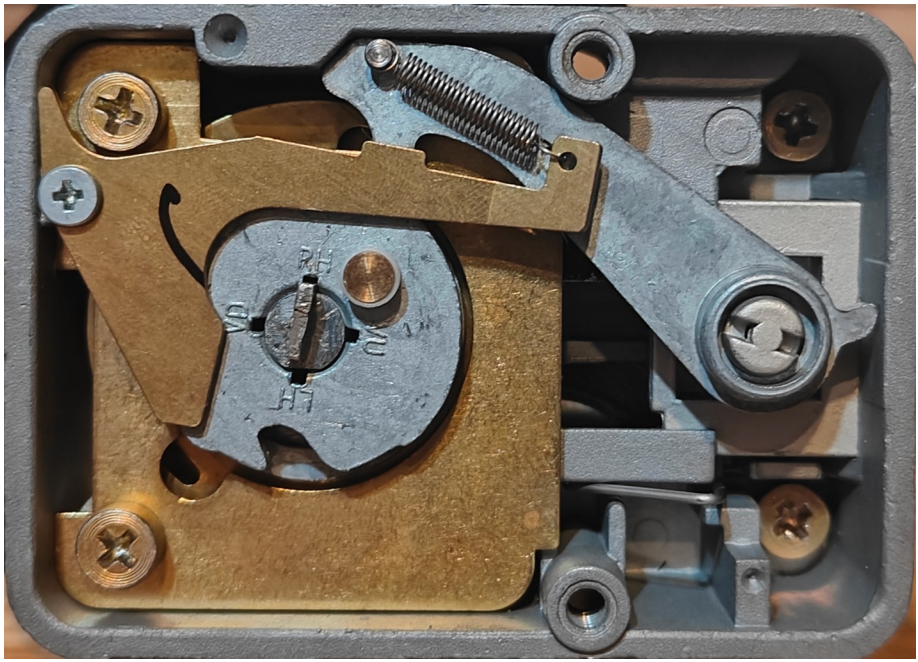
There are some special considerations to consider however. Since you must rotate the dial to reset the assembly, you must make sure you don't disturb the 3rd wheel when you do so. The dial resets the lever at approximately 50 which cuts out half of the available space. The second wheel must also be positioned so that the 3rd wheel's drive pin does not rotate into the fly of the 2nd wheel which would stop it from rotating further. Both of these issues can be mitigated by spinning AWL to park all wheels at 50. This is so that when wheel 3 rotates, it rotates away from wheel 2. After this we start by turning to 0 with a right rotation so as to not mess up the wheels and then push the dial in. Since the 3rd wheel will be rotating right from our perspective, we want to turn the dial right to reset the lever so we don't run into it. With the wheels being parked at 50, we don't want to turn past 50 when resetting the lever. Then we can turn left again to 0 to repeat the whole process.

The amount of wheel travel each time the dial is pushed in, varies. There will be times it doesn't move as well so this must be repeated a sufficient amount of times to ensure that the 3rd wheel has traveled as far as it can. In our case it can only go to 0 since if it goes past 0 we will push it back when we turn to 0. So after we have done this enough to ensure wheel 3 reaches 0, if the gate doesn't align before then, we can rotate past 0 and feel for where it gets picked up. If we feel it at 0 then we know it has not been set yet. Otherwise if we feel it further along then we know it has been set and the number we feel it pick up at is the 3rd number in the combination. In the case that wheel 3 is picked up at 0 we can reset wheels 1 and 2 with left rotation at 50 and park wheel 3 at 0 with right rotation. Now we reset the lever by turning left and turn right to return to 0.

The second wheel can be found in a similar way but along with having to avoid the dial rotation it also has to avoid where wheel 3 is parked.

La Gard 1985

The La Gard 1985 is very similar to the La Gard 3332. The difference lies in the FLCD spring. The spring on the 1985 is more tuned and creates greater difficulty in determining the contact point.



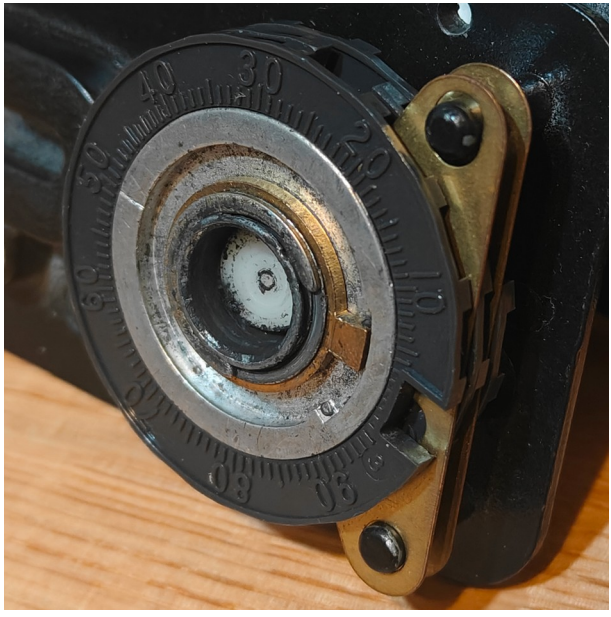
The La Gard 1985 can be manipulated the same way as the La Gard 3332 since they are virtually identical. The contact point is when the fence hits the wheel pack which is indicated by a very slight increase in force needed to turn the dial. More practice will be needed on this versus the 3332 in order to accurately feel the contact point.

Mosler 302

These locks operate the same as a standard Group 2 but is very different inside. And important note is that these also come in Group 2 variants with standard wheels and drive cam. One of the first things you'll notice about the Group 1 Mosler 302 is that it makes a lot of noise when spinning the dial. That's because the drive cam is a shutter drive cam. The wheels are also attached to the back cover of the lock with the lever assembly at the back of the lock body. This doesn't affect dialing in any way. The wheels are also not circular on purpose, they have 16 sides to them and are usually made out of plastic.

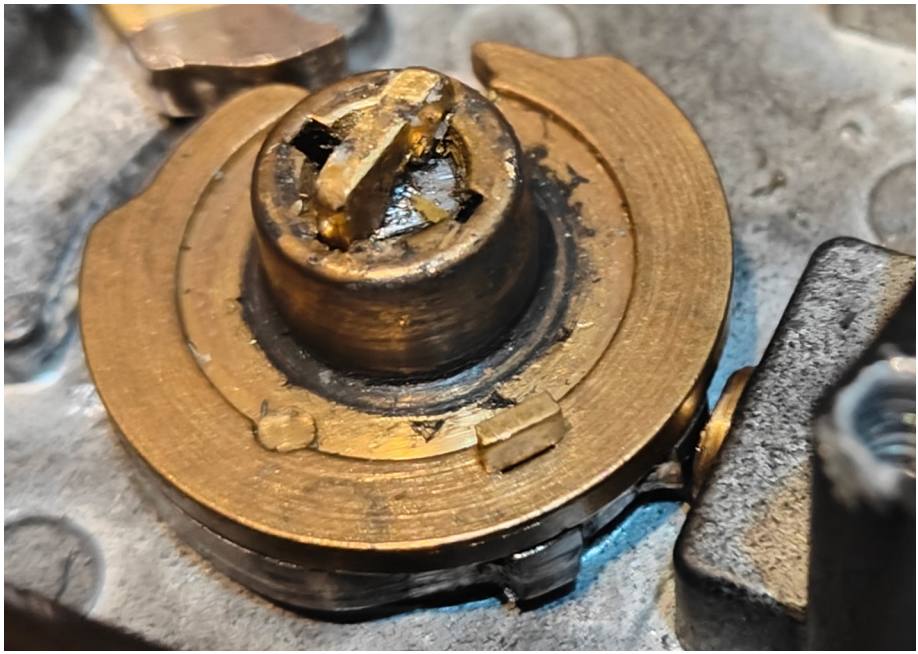
This is the shutter drive cam. It’s split into 2 spring loaded halves with the back silver half having serrations that catch a spring loaded ball bearing. To the left is the ball bearing being pressed into the back half of the drive cam. When it hits a serration, the ball holds the back half of the drive cam in place while the front continues to turn until the spring pressure between the two halves is greater than the spring pressure from the ball and the back half will jump forward to catch up with the front half, bypassing the contact point.

The 16 sided plastic wheels. In the center is a white spring loaded plunger which pressed on the spline key, applying pressure to the dial. This makes it harder to feel for a contact point.

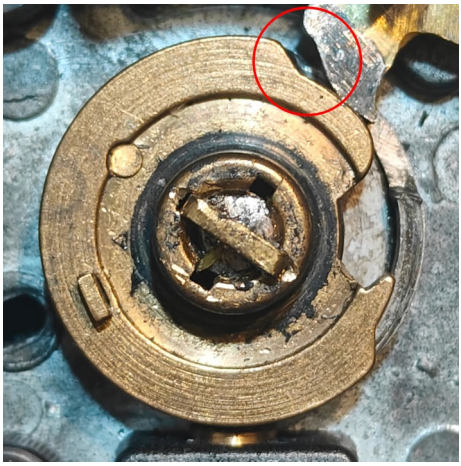


The contact point on this lock can not be felt by a simple turn on the dial. The shutter drive cam springs the drive cam past the contact point and makes it impossible to feel when it happens. However, we can take advantage of a vulnerability in the shape of the serrations on the drive cam. If we balance the drive cam so that one of the bumps is on the ball bearing, turning the dial to just before the drive cam snaps forward, we can rotate backwards (which only the front half) a couple increments, then rotate forwards again. This will bring the contact point to the nose and allow us to feel it.

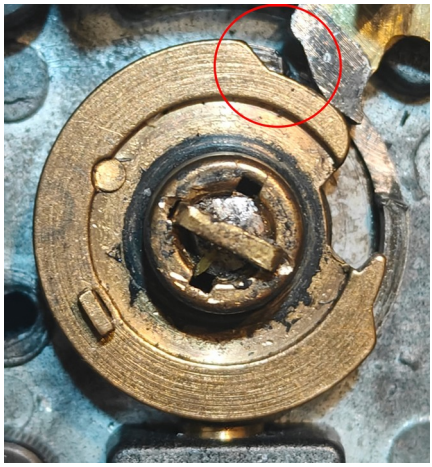
We will want to feel the right contact point since that is going to give the greatest indication due to it's slope. So we start out by turning left until we hear 1 click. That is the first serration going over the ball bearing. Now we want to slowly turn until we hear the second click. Note the exact number as precisely as possible that this happens. Now turn back right to get the ball bearing between the two serrations again and turn left until just before the click. If it clicked at 12.5 then we want to turn to 12.4 if possible, in order to balance the ball on the bump. Below is an image of what it looks like.



The ball has caught the back half of the drive came and is balanced right in the middle of one of the bumps. The drive cam has not turned enough for the back half to catch up with the first.

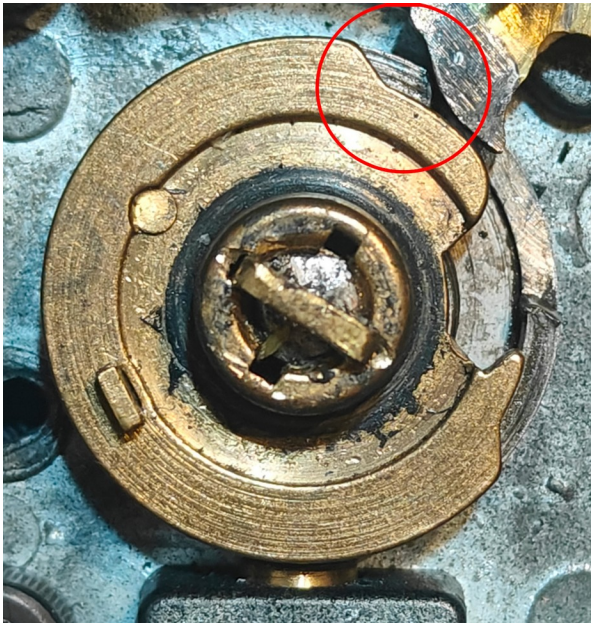


Balanced



Dial turned right

The image above and left shows what it looks like to balance the drive cam. Of course, with wheels, the nose would not be touching the drive cam since the fence would be holding it up. Pay attention to the gap circled in red. At this point you will turn right for no more than 2 increments as shown to the right. You can see the front half has rotated while the back stayed still. This sort of “catches” the back half and from here we can rotate left. Rotating left will move both halves together which will bring the back half towards the contact point and allow you to feel as shown below.



Dial turned back left

You can see that the gap between the back half of the contact point and the nose is gone and they are now touching, giving a contact point. Each step of this process will take a lot of practice to become proficient in. Just balancing the drive cam is hard. And then turning back right and left again to feel the contact point can lead to the drive cam snapping forward.

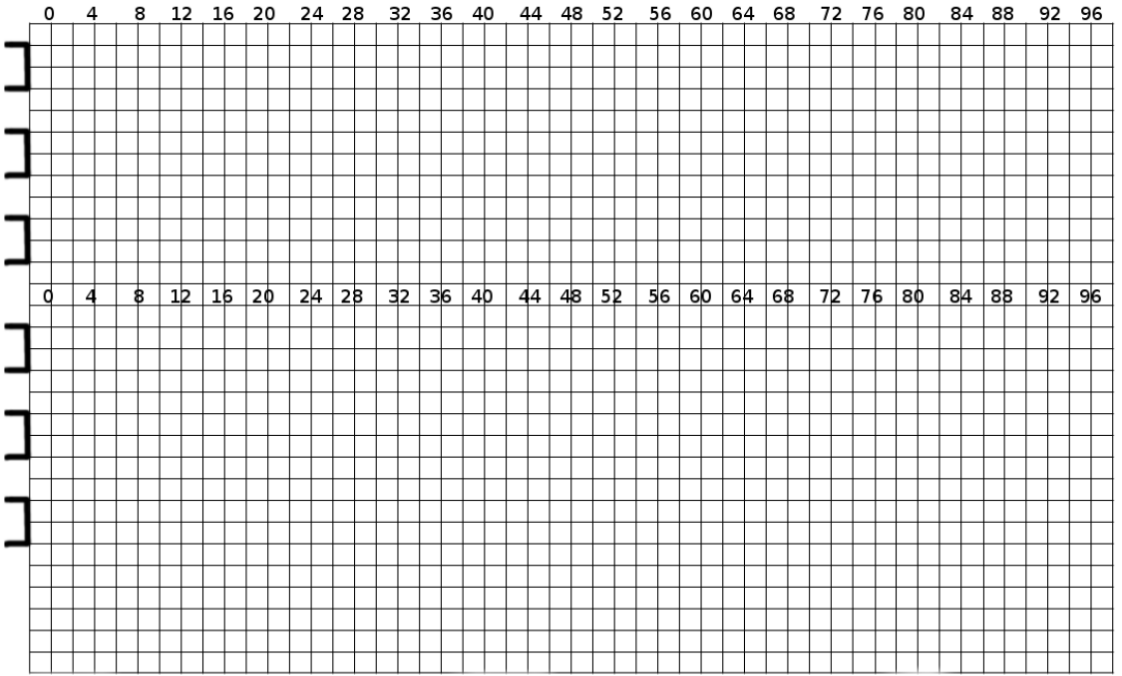
Once the process for taking contact point readings is solid, these can be manipulated the same as a Group 2. But with a 16 sided wheel, it is possible to take a shortcut. Each side is roughly 6.25 increments. So if you make a graph of 10 increments, you can find an edge which will the highest reading and the center of a side will be 3 1/8 increments to either side. This can be extrapolated around the wheel and you then only have to take contact point readings at 16 points around the dial, since a gate is always centered with a side of the wheel. So you took readings every increment from 1-10 and the highest reading was at 4, you can assume the center of one side of the wheels is 7. Then add 6.25 until you get back around so you only have to take contact point readings at 7, 13.25, 19.5, 25.75, etc. instead of 7, 9, 11, 13, etc.

CREDITS

I would like to give a huge thanks to everyone in the locksport community. The method for defeating a La Gard 3330 by finding 3 distinct hills to islolate each hill for each wheel was discovered by Altashot on the forum Keypicking. The method of finding a common low point by taking readings every 10 increments around the dial before starting wheel isolation was discovered by Oldfast on the forum Keypicking. Oldfast is also the person who introduced me to the art of safe manipulation and so I want to give a big thanks for that.

There are also many resources which helped me in my journey. The paper “Safecracking for the Computer Scientist” by Matt Blaze and the book “Guide to Manipulation” by Robert Gene Sieveking were both incredibly helpful.

All images were taken by myself of locks that I own.


0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96
0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96

ABOUT THE AUTHOR

I am a longtime locksport enthusiast. As of the publication of this book, I have been picking locks for around 15 years and manipulating safes for around 12 years. I am also an instructor for locksmiths on safe manipulation and lockpicking. The vast majority of my knowledge has come from other members of the locksport community, publicly available information through online search engines, and my own discoveries. I have a background in cybersecurity which is where my mindset of disclosing vulnerabilities comes from.