Floating Wheels to Cheese Mechanical Safe Locks

by LockManipulator - 2024

1 Introduction

To start with, I'll address the title of this paper. I am using the term "cheese" in a gaming context, which means using a lower skill strategy to defeat a higher skill opponent. Essentially, an easy yet powerful attack that is hard to defend. Traditional manipulation techniques may fail, which would then require a deep understanding of all concepts involved in order to proceed past potential roadblocks. The method outlined here is both easier and more reliable than other traditional methods. It can be written down as a set of steps to follow without needing to understand the intricacies as deeply. And since the reliability is higher, there is less need to be able to adapt on the fly. The skill requirement aspect is also greatly reduced, opening the art of manipulation to a wider audience. This is why I say that we are "cheesing" a lock as well as the fact the the person who brought the idea of floating wheels to me goes by the name of Cheesehead. The phrase "floating" refers to a known effect that happens to the internal wheels depending on the state of the lock. While the principles behind this method do not need to be fully understood, it is still recommended to understand so you may adapt if needed.

The benefits of this method, compared to a standard wheel isolation method, are as follows:

- Being able to choose with nearly 100% reliability which wheel will read first
- Gate indications routinely show ½ increment or more of a change in the contact point (I have personally seen an entire increment drop in the contact point of an S&G 6730, which was in normal working order)
- No need to graph as indications are quite noticeable
- Faster contact point readings as bigger changes can be noticed with less precision
- No need to read the dial with as extreme of precision as 1/8 of an increment
- Bypasses issues of wheel shadowing, even on LaGard locks which are notorious for it

1.1 Requirements

Before diving in, you should already understand how mechanical group 2 safe locks work, along with understanding how manipulation works—specifically wheel isolation. You must understand the principle behind what determines the height of the nose in the contact area and why that matters. The most important aspect is understanding how the wheels move and pick up as this method relies almost entirely on these interactions. For those unfamiliar with these concepts, you may learn more through the book Safecracking for Everyone Second Edition. It's available on Amazon in a hard copy version or in a free PDF. The free PDF can be found by searching for "Safecracking for Everyone part 1" on YouTube and the link will be in the description. The first few videos of that YouTube series also covers the topic.

You should also be able to properly identify your lock. This method varies slightly depending on the geometry of the drive cam in each lock. Drive cams are consistent enough within each brand but vary from brand to brand. On a locked safe, we usually identify a lock by the dial. Therefore, a risk to this method is a mismatched dial and lock body. Thankfully, the two most common lock bodies/dials are LaGard and S&G. Both of which have similar enough drive cams that it makes no difference to this method. Be aware that if you are practicing this on a product called the Challenge Vault by the company Sparrows that the lever arm spring inside these locks is significantly stronger than locks intended to be in use and may hinder your efforts. A strong lever arm spring makes traditional manipulation easier but in this case may cause issues. The possible issue is described in the next section.

2 Floating Wheels

Floating refers to the translation of a wheel on the same plane as it's face. This is not referring to wheels moving forward and back (along the center post) or wiggling along that same axis. This means, when looking at the lock from the front of the dial, the wheels will move up, down, left, and right depending on how we are moving each wheel. The wheel will move perpendicular to the center post.

To imagine this, and to understand how and why the wheels move this way, think of a pole sticking out of the ground. If you put a wheel on this pole, and the inner diameter of the wheel is just slightly larger than the diameter of the pole, it will be able to rotate around the pole. Let's assume the wheel is loose enough on the pole that you have roughly 1 inch of space between the wheel and the pole. If you wish to rotate the wheel and you put one hand on either side you may spin the wheel in place. It does not touch the pole because you are spinning it from two opposite sides of the wheel. However, if you only have 1 hand you may still spin the wheel by pressing against it and pushing it in the direction you want it to turn. In this case you should understand that the wheel will not only rotate but it will move to touch the pole. You may try to lessen this effect by running your hand along the outside of the wheel but the wheel will always be shoved laterally towards the pole due to force being applied only at 1 point.

This effect is what happens inside a safe lock. The wheels can not be a tight fit on the center post otherwise there would be too much friction to smoothly rotate the dial and operate the lock. There must be some degree of "play" between the wheel and center post. In a lock, the drive pins of each wheel are represented by our hand in the previous example and our hand pushing the wheel is the drive pin rotating the next wheel by it's movable fly. This is the only point of contact used to rotate each wheel like in our example. So depending on the direction you are turning and the direction the drive pin is moving, the wheel will move up, down, left, right, or at any angle in between these.

The way these locks are mounted may make it seem like gravity would simply cause the wheels to always be in a "down" position. It may also seem like the fence will push the wheels down when spinning to the contact area. But this does not occur as the wheel pack is always tensioned. That is, each wheel has a spring pushing them together. This tension causes friction which makes it so that if a wheel is moved up, or any other direction, that wheel will stay there until moved again. This wheel pack tension is a requirement for the proper working of a safe lock. Without it, the wheels may keep spinning due to momentum after the dial has stopped and the internal state of the lock will not be as the operator expects it. I have greatly reduced the tension on a test lock and as long as the tension is enough to keep the lock operating properly then the wheels will be able to stay in the vertical/lateral position they are left in. In the absolute worst case scenario, simple gently letting the nose ride the drive cam down to lessen the force the fence places on the wheels is enough to ensure any wheels in the up position remain up.

Now for why this is important. Remember that the vulnerability of these locks lie in the fact that the height of the nose in the contact area informs us of correct numbers in the combination. This is determined by how high or low the fence is which in turn is determined by the "largest" or the highest reaching wheel. If we can artificially push two wheels low and one wheel high then we not only guarantee the high wheel to indicate first but to also have a significantly larger drop for a gate indication than we usually see. This is due to the height difference between the high wheel and the next wheel will be greater than normal.

2.1 Drive Cam Differences

In order to know which direction a wheel is being pushed in we must know the position of each drive pin and movable fly. Thankfully, both S&G and LaGard drive cams have their drive pins close enough to the right contact point that we may simple assume the drive pins of these drive cams are at the right contact point. The drive cam drive pins on S&G locks are almost exactly the same as the right contact point and LaGard is only a few increments away; close enough that we can treat them the same for simplicity. Mosler has their drive cam drive pins 180 degrees away, or 50 increments away. Diebold is 135 degrees away or roughly 30-35 increments lower than the left contact point (as with Diebold the left contact point is the one to indicate more so we will use the left contact point for these locks). From here on out if I refer to a “drive pin” on it’s own I will be referring to the drive pin on the drive cam. If I am mentioning both drive pins on wheels and the drive cam them I will differentiate by specifically mentioning what the drive pin belongs to.

2.2 Getting Our Bearings

On S&G, LaGard, Diebold, and Mosler locks (at least in the last 30 years; I am not an expert in older locks), each wheel has it’s drive pin directly opposite the center of the space occupied by the head of the movable fly. This makes it easy to know which direction each wheel is being moved as it will be the same across the different brands. This also means that the drive cam drive pin, wheel 1, and wheel 3 will always be moved in the same direction as each other. And wheel 2 will always be the opposite of that. The drive cam drive pin picks up wheel 3 by it’s movable fly so wheel 3 will be moving the same direction as the drive cam drive pin. But a wheel has it’s drive pin 180 degrees away from it’s fly. So wheel 2 gets picked up by wheel 3 at a 180 degree offset; moving in exactly the opposite direction. Remember, we are talking about vertical/lateral movement. If Wheel 3 is moving up then that means wheel 2 is moving down. Wheel 2 will pick up wheel 1 with the same 180 offset so wheel 1 will move the same direction as wheel 3 and the drive cam drive pin. So, again, the main takeaway is that the drive cam drive pin, wheel 3, and wheel 1 will always move in the same direction as each other and wheel 2 will be opposite that.

With this in mind, if we know where our drive pin is then we know the direction each wheel is being moved. We are only concerned about vertical movement. As of the time of writing this paper, we can completely disregard any left and right movement. If we were to draw a vertical line splitting the dial ring into a left and right half, whether we are moving a wheel up or down depends on the direction of rotation and which half our drive pin is on. As an example, if we are turning the dial left and the drive pin is on the left side then the drive pin, wheel 1, and wheel 3 are moving down and wheel 2 is moving up.

3 Manipulation

This section assumes you already know how to perform a full manipulation using wheel isolation. Unfortunately, I am unable to find in depth video resources for this at the moment but the book Safecracking for Everyone Second Edition covers this quite well. The Safecracking for

Everyone YouTube series does touch lightly on the topic in later videos but is not as in depth as the second edition of the book. We will be modifying traditional wheel isolation methods, such as completely excluding the process of finding common low points across each wheel, while staying true to the core principles of wheel isolation. If you understand the older AWL method and how wheels move, then in short, wheel isolation is simply only having 1 wheel change position in between contact point readings.

To start with we should now already know the following:

- Our lock model
- Our right (or left for Diebold) contact point
- Where our drive pin is based on the above
- Our contact point, drive pin, wheel 1, and wheel 3 all move in the same direction
- Wheel 2 moves opposite of the above

Our process, using this information, will be as follows:

1. Park wheel 1 and wheel 2 in a downward direction
2. Isolate wheel 3 only in the up direction
3. Keep or re-park wheel 1 in a downward direction and isolate wheel 2 only in the up direction
4. Brute force wheel 1 to open the lock

3.1 Parking Wheels

The first step is the new equivalent of finding a common low point across all wheels in order to keep our static wheels from shadowing the gate of our isolating wheel. But instead of taking time for multiple precise contact point readings we already know where to park each wheel. Down of course! Wheel 1 is always set first. It’s not a requirement, but let us respect each wheel’s rotation in the combination and spin left to pick up wheel 1. Since we are spinning left, the drive pin (and thus wheel 1) will be moving down while it’s on the left half of the dial ring. So after we pick up all of our wheels we can stop when the drive pin is at the 9 o’clock position (the dial will read 25 increments higher than the drive pin location) and wheel 1 is now parked with a down direction You can stop at any point when the drive pin is on the left half of the dial ring. I choose the 9 o’clock position as that is when our applied force is directly downwards to try and get the most movement and reliability. The further from the top/bottom we are, the better. Although up and down movement is still passed on close to the top/bottom, there will be more lateral than vertical movement. I will use an S&G 6730 with a right contact point (and thus drive pin) at 7 for an example. For this I would spin left to pick up all the wheels and stop at 32.

To park wheel 2 in a down direction we must first pick it up. Turning right until we pick up wheel 2 we will already be moving wheel 2 in a down direction since we’re turning right and the drive pin will be on the left half of the dial ring when we pick up wheel 2. We only need to move it a few increments to ensure it has been moved down. I tend to round down to the nearest multiple of 5 for simplicity although if that is only 1 or 2 increments away then I will spin to the next multiple of 5. In my case, I would take wheel 2 to 25 with a right rotation but 30 would be an acceptable choice as well.

3.2 Isolating Wheel 3

From this point, unlike traditional wheel isolation, we can not simply turn left 1 rotation to pick up wheel 3 and move it 2 increments further to take a contact point reading. This is because the moment we pick up wheel 3 with our left rotation, our drive pin will be moving down. This is not good! Instead of thinking of left/right rotation for setting wheels, we should start thinking about up/down direction. We have to ignore how each wheel turns in the combination. This also means we may find a number for a wheel with the “wrong” rotation. We can simply apply rotational conversion if we need to set a wheel on a number with the wrong rotation. If you are lazy and trust your precision in dialing then simply turning past your target number by 1 increment should keep you within tolerance; provided that your target number is the exact center of a gate (this is incredibly risky and I do not recommend this).

A short explanation of rotational conversion is that if you spin all the wheels left to 0 and then spin all the wheels right to 0, the dial says 0 in both cases. But the wheels will be in different places due to the thickness of the drive pins/movable flies. The flies are movable to offset this but it’s not perfect so there’s still an error that compounds through the wheels. Setting a wheel with the wrong direction means we must spin an extra amount further. This amount is different for each wheel and you can find yours by setting all wheels to 0 with a left rotation and feel how far off each wheel picks up with a right rotation.

After we pick up wheel 3 with left rotation we want to keep spinning until the drive pin starts to move up. That is when the drive pin reaches the very bottom of the dial ring (since we are turning left) which is also when the number on the dial reads 50 away from our drive pin. Keep in mind that because we parked wheel 1 and wheel 2 roughly 90 degrees (25 increments) away from our drive pin, we are skipping over approximately 25 increments. We will come back to that later. Since my drive pin is at 7, I will turn wheel 3 left until the dial reads 57. I like to manipulate every 2 increments and on even numbers so I will turn one extra increment to 58. Now I may turn to my contact point and take a reading. From here we may proceed as if we are doing a normal wheel isolation for wheel 3. We advance wheel 3 by 2 increments after each contact point reading. But unlike normal wheel isolation we do not go until we get back to wheel 2. We only go 50 increments (once we reach our drive pin) since that is when the drive pin passes over imaginary left and right divider of the dial ring and into the left half; changing from an up direction to a down direction. For my example, I will isolate wheel 3 from 58 to 6. In an ideal scenario we know the third number in a combination can not be in the contact area so theoretically we can stop at the left contact point and eliminate around 10 numbers, or 5 readings, and save time.

Do we now go back and isolate through the numbers we missed at the start (which would be from 26 to 56 in my example)? Not yet! We want to first worry about the numbers ahead of us (8 to 24) that we didn’t do because we stopped early due to not wanting to move wheel 3 downwards. But we can’t do so with left rotation as this would be pushing wheel 3 down. If left rotation moves a wheel down through an area then a right rotation moves that same wheel up through that same area. We must rotate right through this area so wheel 3 is pushed up for our contact point readings.

To do so, we will simply keep turning wheel 3 left all the way to 25. We had set wheel 2 on 25 earlier but we don’t actually have to worry about bumping it because we set it on 25 with a right rotation and here we are dropping wheel 3 off at 25 with a left rotation. Because of rotational conversion, right 25 is approximately left 25.5. So as long as we are careful not to go past 25 at all then we should be safe. But you may stop at 24.5 if you are worried. We want wheel 3 to be all the way at the end of our isolation zone so we can turn right 1 rotation and pick up wheel 3 and isolate it through this end area in the up direction. Now that we have wheel 3 in a right rotation we can get our contact points for, in this example, 24 to 8.

Now we can take readings for the numbers at the start that we skipped. We already took readings for 58 through 6 so we can spin wheel 3 past all those and start taking contact point readings at 56 and continue until we get back to wheel 2 at 25 (in my case 26 would be my last reading as I use even numbers only). We now have a full set of readings for wheel 3 every 2 increments and all in an up direction and should have found our gate for wheel 3. Hopefully you got a much bigger indication than you're used to! Since I don't graph, the way I amplify a gate signature is as soon as I get a drop I take readings for the two increments which will tell me the center of the gate as gates are usually 3 numbers wide. If the reading goes up again immediately I know the drop was at the edge of the gate and I can choose 1 increment back as the center.

3.3 Isolating Wheel 2

Wheel 2 will be isolated in a similar manner to wheel 3. It's important to note that I did many tests running wheel 2 and wheel 3 together to save time from having to re-set wheel 3 to it's gate. This can work because if we are moving wheel 2 up then wheel 3 is being pushed down. However, this is not 100% consistent. And when it does work we may only get ¼ of an increment change in the contact point instead of the ½ increment change we are hoping for with this method. So while this *can* significantly speed up a manipulation, it may also yield no results on wheel 2.

To begin isolating wheel 2 we can re-set wheel 1 in a down direction or just pick up wheel 2 and bring it with a left rotation to where wheel 1 was parked. Either way, you will be picking up wheel 2 with a right rotation from this point. For me that is picking up wheel 2 at 52 with a right rotation. We can't immediately begin our contact point readings as our drive pin is moving up on the left half of the dial ring meaning wheel 2 is moving down. So we will skip past numbers and rotate until we get to our drive pin (7 for me so first reading will be at 6) and then we can start. Just like wheel 3 we will take our first set of reading for only 50 increments which is when the drive pin crosses to the right side and starts moving downwards (my last reading would be 58 in my example). If you choose to re-set wheel 3 on it's gate before each reading, we don't have to worry about the vertical direction as the gate will be under the fence. If for some reason you didn't find a gate and only a low point then you should put wheel 3 on it's low point in a downwards direction.

And just like wheel 3, once you reach the end of the downward section you will keep rotating wheel 2 until you reach where wheel 1 is parked (32 in my case). Then rotate left until you pick up wheel 2 and take readings for the numbers you missed at the end. Once you get back to the numbers you already took readings for (6 through 58 for me), spin past all of them and get readings for the numbers you skipped at the start (8 through 32 for me).

3.4 Isolating Wheel 1

Out of the dozens of manipulations across almost 20 different locks of mixed brands and models that I have done using this method I have not needed to isolate wheel 1 in respect to it's up/down direction (besides when attempting to spin wheel 2 and wheel 3 at the same time instead of isolating wheel 2). But in the event that you wish to do so, isolating wheel 1 is the simplest of the three wheels. You start with your drive pin at the bottom of the dial ring (the dial should read 50 increments away from your drive pin). Spin right from the drive pin + 50 to isolate half the dial and spin left from the drive pin + 50 to isolate the other half, re-setting wheel 2 and wheel 3 on their gates/low points (keeping in mind up/down direction if they are low points and not gates).

3.5 Shortcut

If this is all a bit complex, there is a shortcut that makes it extremely easy. If you already understand how to isolate wheels, then the only extra knowledge you need is where your drive pin is at. In my testing, I have found that wheel 3 does not affect the contact point much whether it's going up or down. Wheel 1 has the greatest effect with wheel 2 being in between. So to simplify the process, you can replace finding and using common low points with this rule of thumb: Park wheel 1 with a left rotation 25 increments above the drive pin and wheel 2 with a right rotation 20 increments above the drive pin. Then isolate wheel 3 as normal, starting from where you parked wheel 2. This also means that you will only be spinning wheels as they spin in the combination and won't need to use rotational conversion.

This is much easier to understand while still reliably forcing the wheels to read in the order of 3-2-1. The downside is that you might only get the standard ¼ increment drop in your contact point for a gate indication instead of more. This means you should still try to be as accurate as possible in your contact point readings. The time difference in dialing between the shortcut and the full method is negligible.

Pros

Easy to understand
Wheels are still forced to read in the order of 3-2-1
The gate of a wheel will be found in the same direction the wheel spins in the combination

Cons

May only have ¼ increment drop instead of more as this method was originally designed to do

4 Cheatsheet

Definitions

L = Left
R = Right
RCP = Right contact point
w1/2/3 = Wheel 1/2/3

S&G/LaGard drive pin = RCP (technically LaGard drive pin = RCP + ~5)
Diebold drive pin = RCP – 32.5 (technically LCP)
Mosler drive pin = RCP + 50

If RCP + 50 is over 100, subtract 100
If RCP – 32.5 is under 0, add 100

If you set a wheel on a gate/low point with a different rotation than it was found, use rotational conversion!

Shortcut method

1. Park w1 L @ drive pin + 25
2. Park w2 R @ drive pin + 20
3. Isolate as normal

Full method

Isolate w3
1. Park w1 L @ drive pin + 25
2. Park w2 R @ drive pin + 20
3. Pick up w3 L and isolate from drive pin + 50 until reaching the drive pin
4. Continue turning w3 L to w2 (don’t bump w2)
5. Isolate w3 R from w2 to drive pin
6. Continue turning w3 R to drive pin + 50
7. Isolate w3 R from drive pin + 50 to w2

Isolate w2
(Re-set w3 before each reading)
1. Park w1 L @ drive pin + 25
2. Pick up w2 R and isolate from drive pin to drive pin + 50
3. Continue turning w2 R to w1 (don’t bump w1)
4. Isolate w2 L from w1 to drive pin + 50
5. Continue turning w2 L to drive pin
6. Isolate w2 L from drive pin to w1

Isolate w1
(Re-set w2&w3 before each reading)
1. Isolate w1 L from drive pin + 50 to drive pin
2. Isolate w1 R from drive pin + 50 to drive pin

4.1 Acknowledgments and Final Words

I appreciate Jan-Willem for bringing the phenomenon of floating wheels to my attention. I also want to thank Cheesehead for explaining why this happens and pushing me to put it to use. I have also been made aware that utilizing floating wheels is not new and that this is a rediscovery. So to “cheese” a lock may not be the first name given to techniques which purposefully float wheels during manipulation. However, I do not know the extent at which this is/was used in manipulation nor do I know how common it is in other parts of the world. I have been exposed primarily to manipulation in the U.S. which has sadly lost much knowledge over the decades due to tradesmen picking other skills such as drilling over manipulation.

Last edited Jan 2, 2025