Picking Abloy Classic - Theory and Practise

Matt 'The Lock' Smith 2016

Aka HuxleyPig

citadellocktools@hotmail.com

Contents

Introduction

Locksmithing goes back a long way in my family. If you count my mother working as a receptionist at Josiah Parkes and Sons, Willenhall it has been in the family seven generations.[1] Everyone before my mother were locksmiths at the same factory.

Whilst my background is primarily in software development, security has always been an interest of mine and physical security seemed like a natural progression from IT security. So it followed that I too became a locksmith.

Influences and Motivations

There is a legendary toolmaker known as John Falle. Whilst perusing LSS+ about 13 years ago, I came across a video in which he describes his Abus Granit pick. The interviewer asks him if the principle can be transferred over to the Abloy, to which Mr Falle declares that it was impossible, going on to explain why. I now know this as "The Problem 50 Paradox" and is covered in the text below. From pretty much that point onwards it became a lock that I simply had to defeat; a burning ambition that became like a worm boring into my brain. Because *nothing* is impossible.[2] Incidentally, Falle developed a wire decoder/make-up key for the lock instead.

Locksport folklore is littered with veiled references to half-forgotten tools from yesteryear that have since taken on mythical status. One such example is from the 70's and is known as the 'Vempele',[3] which lead Abloy to making a design change to their lock specifically in order to defeat the tool. Unfortunately, legend also has it that the tool was wielded by a particularly nasty sex pest, who most definitely used it for evil.[4]

Since then the lock had allegedly gone unpicked.

The advent of the internet has unearthed many attempts to create a tool for the lock. From the many examples that I have seen, none satisfy Problem 50 and as such there has never been a tool publicly available that works. There are examples of tools that allow the lock to be set from back to front but the author has never seen this technique successfully employed on an actual Abloy.[5] Should the lock **not** happen to bind up perfectly from back to front, or if there are false gates present, then the tool will not work. Having the ability to traverse through the disc pack at will is essential.

It is the author's intention to highlight the many obstacles that had to be overcome in order to design a picking tool for this lock. The difficulty of realising said design is out of scope and not covered here.[6]

[1] Although I admit this is a bit of a stretch.
[2] Within reason.
[3] Finnish for contraption, or thingamajig.
[4] Please, please, do not use the information contained herein for evil.
[5] Only on cheap knock-offs.
[6] But was probably tougher than the design, for reference.

Lock History

In 1907 a Finnish company designed the Abloy lock. Using rotating discs, its design was revolutionary for the time. Having no springs, the lock was remarkably durable and especially suited to the inclement climes of Finland.

Abloy grew and during the 1960's offered a reward of 1 million Finnmarks at their factory in Joensuu if someone could open the lock without damage or prior knowledge of the lock.[7]

Since then Abloy have been bought out by the multi-national conglomerate known as Assa-Abloy and are synonymous with 'high security' to many happy customers. Their current flagship lock, the Protec 2, is rated as one of the hardest locks to pick on the planet. Abloy still sell the Classic in several forms and the lock is still present 'in the wild' in massive numbers, especially in Finland.

[7] Maybe <citation required>.

The Chinese Aberration

Not long after the turn of the century, a company from China called H&H made a tool for the Abus Granit. It was a poor copy of a tool already being sold by Jaakko Fagerlund[8] [9] but because of this, at least it worked. At some point during the development process someone had the same idea as the interviewer in John Falle's Abus tool video; namely to apply the same concept to the Abloy Classic.

Another locksport urban myth is that the testing team of H&H reported back to their superiors that the Abloy tool simply did not work as intended and that the Abus principle simply was not applicable. However, in spite of this, H&H went ahead and produced the tool in massive numbers. They still do to this day.

This may well be a case of 'animation overruling intelligence' as demonstrated by the following Youtube video:

https://www.youtube.com/watch?v=w8eo107h3H8

Walker Locksmiths still sell this useless thing (amongst many other vendors) in the full knowledge that it does not work, for the princely sum of £90.00!

The author paid £100.00 GBP for his H&H Abloy tool and it has never opened a lock in its life. Not only does it not satisfy Problem 50 but should the lock contain any anti-pick discs (detailed later) then it is, again, completely useless. This also fuelled my drive to make a tool that **did** work.

It is the author's opinion that H&H should refund everyone who has paid good money for this thing.[10]

Fig 1.1 H&H's useless Abloy pick.

[8] A great Finnish toolmaker and hellraiser.
[9] Which, in turn, was a good copy of Falle's tool.
[10] Interestingly, Falle was given this tool to see if he could improve on it but thought it was impossible, and beyond even him.

Lock Breakdown

The Abloy Classic contains between 7 and 11 discs, depending on the specific lock.

Fig 2.1 A selection of Abloy Classic locks.

Each disc has 6 possible cuts over a 90° range, thus giving 18° per cut.

Fig 2.2 The six possible Classic gate positions.

The discs are separated by 0.55mm washers in order to guarantee independent rotation and have tabs on the top of them to limit their movement to 90°.

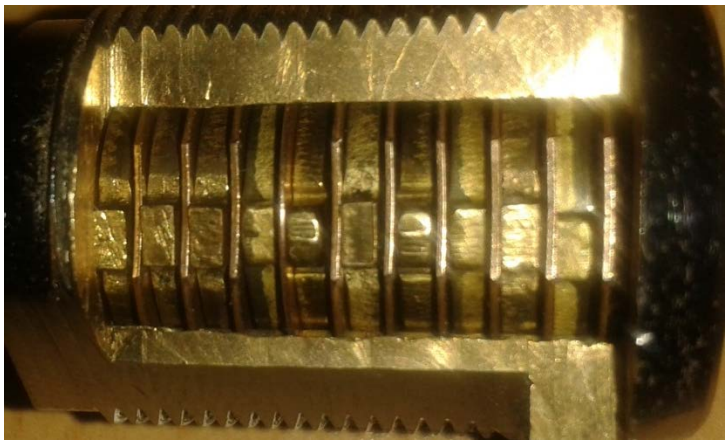

Fig 2.3 The disc pack, their tabs and washers.

The key has angular cuts corresponding to the position of the gates.

Fig 2.4 Abloy Classic key.

If the correct key is inserted then all of the gates will line up, allowing a sidebar to retract into them and thus the plug is free to rotate.

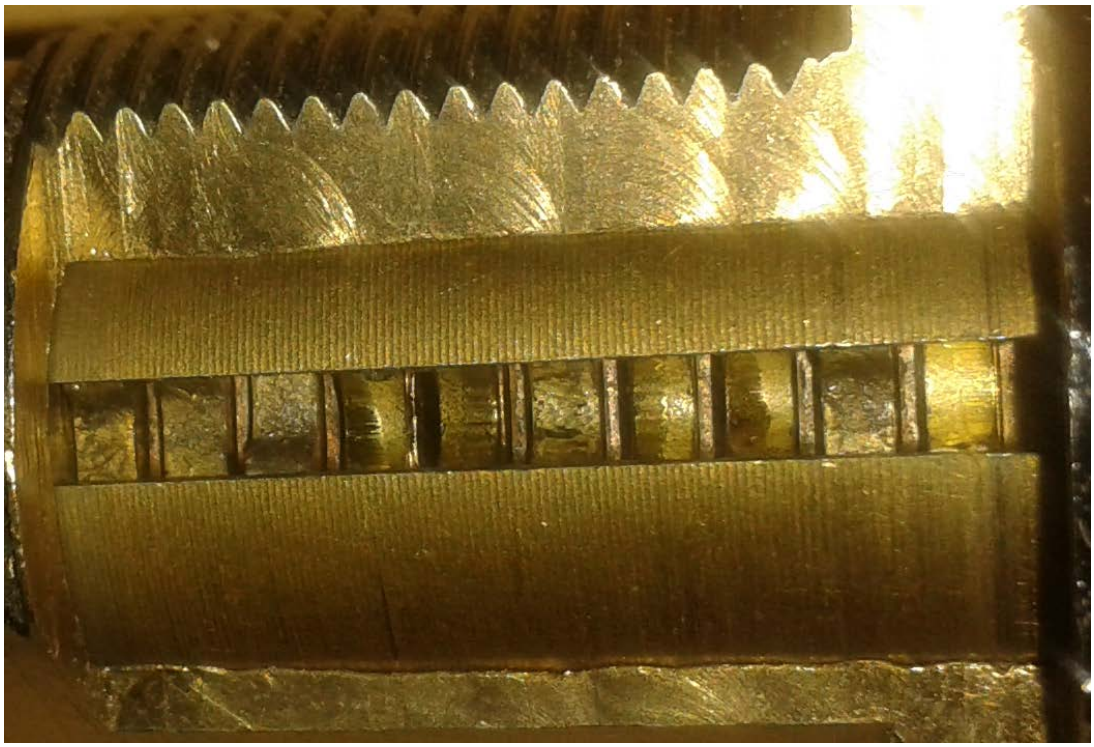

Fig 2.5 The gates when lined up correctly.[11]

[11] Sidebar removed for clarity.

The Theory of Picking Abloy Classic

Standard lockpicking theory tells us that so long as there is a physical barrier blocking the rotation of the plug, then there has to be a binding element somewhere inside the lock. It is this basic premise that, should the user have access to manipulate said binding element(s), allows us to pick locks. Add into this the inevitable manufacturing inaccuracies and the lock then becomes eminently pickable.

This premise holds true for Abloy Classic too; should an attacker be able to apply tension to the mechanism and then individually manipulate the discs, then the lock should be pickable.

Specific Barriers to Picking

Constricted Keyway

The key has a diameter of 6mm, which is cut in half to form a semi-circle with a height of 3mm. So from the beginning, there is only 3mm to work with. Furthermore, the lock can be in a position such that only 90° of the keyway is available, again halving the working space down to just 90° of a 6mm diameter circle.

Fig 2.6 The 90° of working space.

Any potential tool is going to have to exist and operate within this space.

Off-Centre Axis of Rotation

This aspect of the lock's design makes designing a tool especially difficult. Any potential design would have to rotate *around* the centre of the lock. Most disc detainer tools that exist have their axis of rotation as the centre of the lock and so tool design is simplified.[12] In this case, every aspect of the tool has to completely avoid the centre of the lock because only 90° of it is ever available.[13]

[12] Such as the Abus Granit tool.
[13] Another aspect that H&H failed to address.

False Gates

It seems that Abloy were well aware of the potential for their lock to be picked from the very beginning. False gates are present inside every lock I have looked at, which can only exist to confuse and frustrate a potential lockpicker.

The false gates take the form of shallow cuts around the edge of the disc. More modern examples have multiple false gates, differing in both depth and shape in order to obfuscate further.

Fig 2.7 A close up showing real and false gates.

Free-Spinning Front Disc

The front disc in the Abloy Classic was *always* a 0 cut.[14] Therefore it could be used to tension the lock. The Vempele tool mentioned above made use of this fact. Because the front disc was easily accessible, the Vempele only had to have one component exist inside the 90° of space mentioned previously.

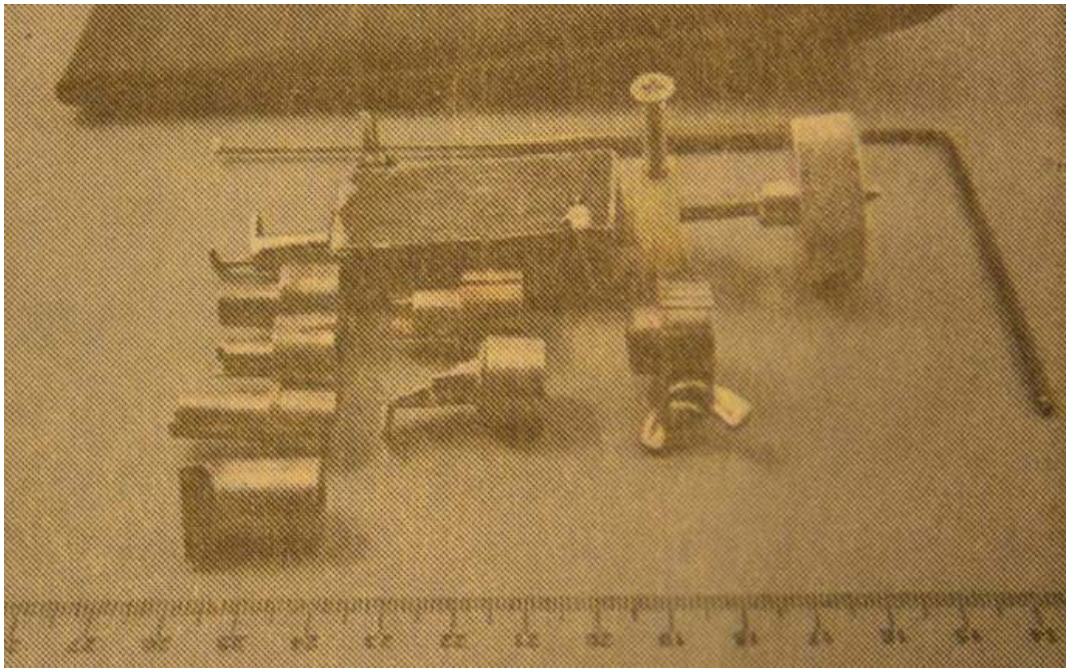

Fig 2.8 Grainy police photograph of the Vempele.

Abloy combatted this by removing the movement-restricting tab from the front disc (resulting in a free-spinning disc) and (in some cases) making it from steel. This served a dual purpose; to stop the lock being tensioned from the front disc and also to provide drill resistance.

Removing the tab made it so that the disc could be rotated into a position whereby the key could not be inserted into the lock but as it was the outmost-facing disc it could easily be rotated back into the correct position using the tip of the key. It is for this reason that the tabs cannot be removed from any other disc because should that disc slip round too far then the lock would be made inoperable.[15]

The result of this change made it so that in order to tension the lock, an attacker would have to use the *deepest* disc, which was, again, always a 0 cut. A 0 has to exist inside of the mechanism *somewhere* in order to drive the plug round with the correct key inserted.

From a tool-design perspective, this makes it necessary to have both the tensioner **and** the pick arm/head share the same restricted space; a much tougher prospect.

[14] Up until the relatively recent advent of the 7 disc camlock.

[15] Unless the tabs were removed from every other disc in front of it, going all the way to the face of the lock. If the tabs were to be removed from *every* disc then the lock would spin uselessly, even with the correct key inserted, in the Abloy Classic design.

Anti-Pick Discs

At some stage, Abloy introduced a modified disc into their locks. This disc took the following form:

Fig 2.9 Anti-pick disc.

The extra cutout in the centre is designed to foil picking implements. If the tool does not have an (almost) full profile then any rotation of it will enter the cutout instead of turning the disc. This is yet another reason why the H&H tool is a waste of time.

Fig 2.10 The tip of the H&H tool being defeated by an anti-pick disc.[16]

[16] Note that even without anti-pick discs, the H&H tool does not work.

The Problem 50 Paradox

Whilst related to the restricted keyway, this issue provides the single largest barrier to making a locktool. As a thought exercise it is, as Falle correctly stated, impossible to defeat. Luckily, reality does not tally up to the theory.

If an Abloy Classic has both a 5 cut (90° removed from the key) **and** a 0 cut (nothing removed from the key) in the same lock then it is impossible to set the deeper of these discs without disturbing the other, shallower disc. To set both of these discs would require 90° of movement, which would be ok if the picking arm were invisible but said picking arm has to exist *somewhere,* meaning that it has to exist within this 90° range. Therefore, it is impossible to rotate the full 90° without hitting a 0 or a 5 disc in front of it (and thus nudging it out of position).

Fig 2.11 The maximum range of travel allowed for the Abloy Classic.

There is another aspect to this problem that exhibits itself when trying to manoeuver from disc to disc. The picking head needs to be thin enough to slip into the 0.55mm gap created by the washers. If the picking head were any thicker it would be impossible to leave a disc in the correct position; instead the disc would need to be at the same rotation as its neighbour, which is obviously useless.[17]

The author has spent longer designing around Problem 50 than any other. It seemed that all of the previously mentioned challenges were surmountable with clever design. All manner of solutions from flexible materials to miniature gearing have been considered before finally arriving at a solution. As previously mentioned, Problem 50 is a paradox whose rules are seemingly impossible to defeat. Serendipitously, the rules of this game can be…*bent* a little.

[17] Unless the cuts happen to be the same, which can't be the case for the whole lock.

The Practise of Picking Abloy Classic

As with the traditional pin tumbler, certain tolerances are exploited by would-be attackers. If a tool could be conceived that satisfies all of the above problems then the picking of the lock suddenly becomes a distinct possibility. In reality, it is still not *easy…*but possible.

Specific Solutions to Picking

Careful study of the lock has revealed some nuances that can be exploited through careful tool design and technique.

Constricted Keyway

Only having 90° of a 6mm diameter available is not much room. In this space there has to be both a tensioner arm and a pick arm. The proportions of which depend on how much strength is required. Giving the tensioner more of the space makes it stronger but conversely, it makes the pick arm weaker.

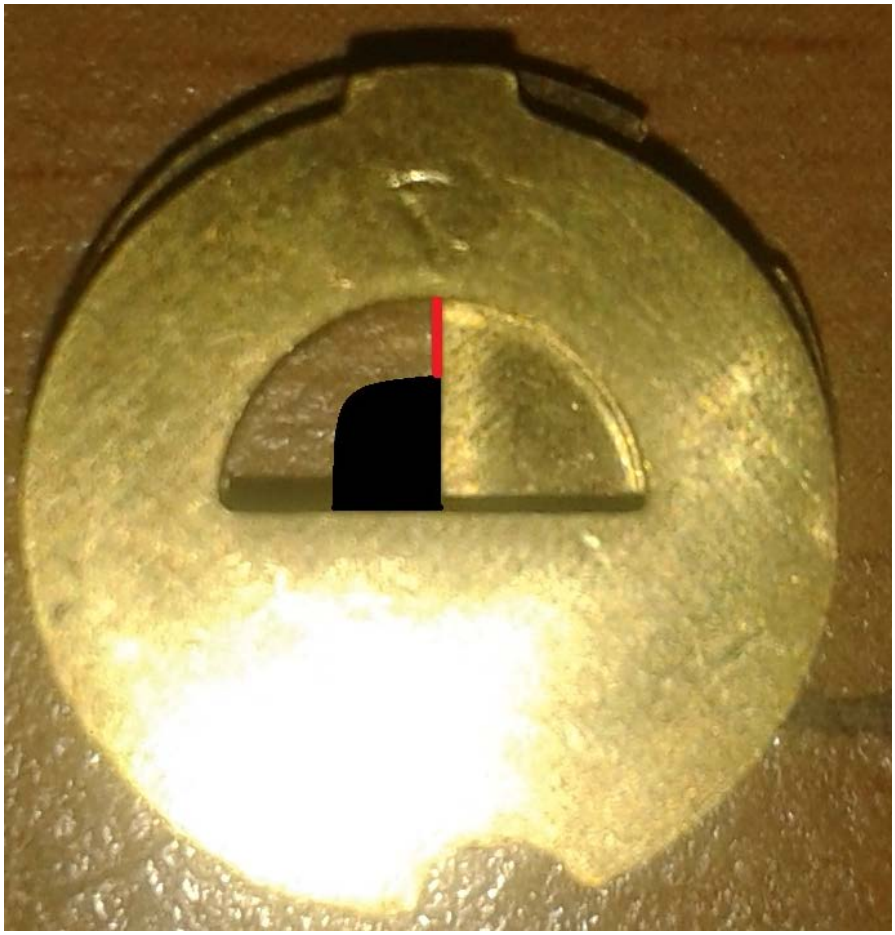

Fig 3.1 Approximate dimensions of tensioner (black) and pick arm (red).

In this way, the tensioner arm always stays within the 90° space (because it does not move) and the pick arm *almost* manages to stay within it too, which we will cover later with the Problem 50 Paradox.

Off-Centre Axis of Rotation and Free-Spinning Front Disc

Having off-centre tooling is similar to a crankshaft on a car. So long as there is some part of the shaft that is rotating concentrically then the off-centre parts will be free to move around their axis too.

Fig 3.2 An early prototype showing the tensioner and picking arm.

In this fashion the free-spinning front disc is ignored (as far as tensioning the lock is concerned) and is set by the pick head instead. The deepest disc is used to apply tension to the mechanism whilst the pick arm moves around the edge of the disc circumference.

False Gates

These are dealt with by way of technique, similar to security pins found inside pin tumblers. When picking the lock, all of the discs are placed into *a* gate, whether real or false. At this point the discs will bind up quite hard. Then, go through the disc pack and give each disc a 'wobble'. There will be one disc that will be binding very hard and will not wobble as much. This disc will be in a false gate and will need moving. Sometimes it is necessary to come off the tension a little in order to free the disc. When the disc is move to the correct gate it will once again take the characteristic wobble and the next false gate can be dealt with.

This does require a certain amount of skill but any lockpicker with a little experience should pick this up very quickly.

Anti-Pick Discs

As previously mentioned, many tools have succumbed to this particular defence. The author is unaware of when Abloy introduced this countermeasure but it is fair to assume that it was as a direct result of a potential attack, in a similar fashion to the Vempele, and the free-spinning front disc. Indeed, maybe the anti-pick discs were inspired by the same attack. Upon careful examination, the Vempele does look like it could have exploited this.

The cutouts are 3.5mm diameter, leaving 1.25mm on each side for the key (or any tool) to operate on. Thus, anything less than an *almost* complete profile will result in not being able to manipulate the discs at all, or being limited to uni-directional operation only.

The author created a tool called 'The Ablator' (covered in more detail below) that uses a full profile for its picking head. This avoids the anti-pick discs and allows bi-directional movement of the head.

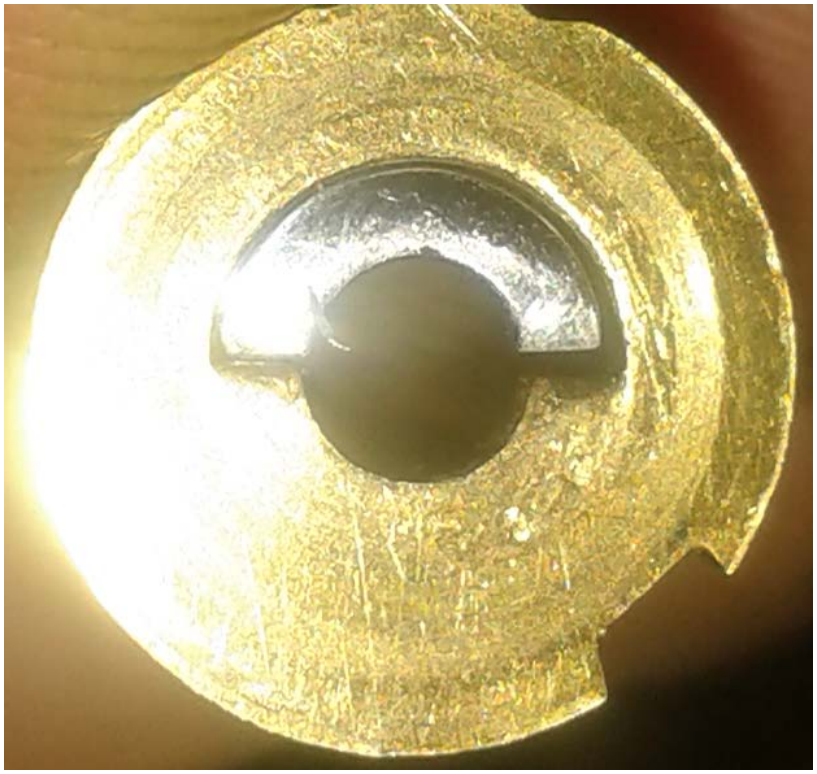

Fig 3.3 The picking head profile of the 'Ablator'- The Abloy Classic pick- avoiding the anti-pick discs.

The Problem 50 Paradox

When the lock is under tension, what is actually happening? Well, the sidebar is being pressed down onto the discs and depending what part of the disc is being presented to the sidebar will dictate what happens.

Let us pretend that there are only 2 discs inside of the lock. We use the rearmost disc to tension and manipulate the second disc in order to pick the lock. What if the disc is not *quite* aligned properly when tensioned? What happens? In the example pictured below, the tension can be visualised as a downward force onto the disc from the sidebar.

Fig 3.4 Round sidebar misaligned with round gate.

If it is still not clear, a slightly misaligned gate will still move round to its correct position when tensioned because the sidebar will push down into the gate and move the disc on its own. In a nutshell: **so long as > 50% of the sidebar is overhanging the gate, the lock will still open when tensioned. You can get away with disturbing the discs, just a little.**

This holds true for the whole disc pack and therefore bends the rules of The Problem 50 Paradox; now we have more like 102° - 112° within which to work. Enough space to accommodate a thin pick arm.

The exact amount of extra rotational room is dependent on the model of Abloy Classic. As a rule, the rounder the sidebar and the rounder the gates, the larger the amount of allowable rotation. The minimum allowable amount the author has found is 6° in either direction, equalling an inclusive 12° minimum allowable overextension of the discs.

In addition to this, there is a certain amount of 'slop' within the lock. Tolerances that have to exist in order for the lock to function smoothly, even with a little wear. Although small, it is significant and serves to give a little more breathing room.

Later designs of the lock featured a change to the shape of the sidebar and the gates. This suggests that Abloy were well aware of this issue because they squared-off the gates and made slimmer, oval shaped sidebars. This serves to cut down this effect. Indeed, later models of Abloy use an almost rectangular sidebar. Unfortunately for Abloy, their efforts were not enough to make the lock unpickable.

Fig 3.5 The later squared-off gate and oval sidebar.

There is also a technique-based solution that helps with Problem 50; if a disc binds and is a 0 or a 5 then the pressure from the sidebar is often enough to keep it sufficiently (mis)aligned anyway. So disturbing it with the pick arm becomes somewhat difficult. A non-binding disc is still easily disturbed, however.

The Ablator

The locktool that was ultimately spawned from all of this is called The Ablator.[18] It has undergone many revisions, is still evolving and will undoubtedly undergo many more. A tool is never 'complete', only in its latest state of metamorphosis. At the time of writing the tool is at V2.6, a picture of which is shown here.

It is a pick/decoder, so once the lock has been picked, a code can be derived and a key cut if required. This is done by reading off the code from the engravings present on the handles.

Fig 4.1 Version 2.6 of The Ablator.

Until it had satisfied a 'Problem 50 worst case scenario' I was not happy to unveil the tool. This scenario was a lock that had been coded thus: 05050505050, which it happily picked.

The technical challenges involved in making a tool such as this are many and not covered here. Suffice to say that having to make this by hand takes a very, very long time. Because of this, the author sells this tool but they are not 'cheap'. [19]

Please address any enquiries via the email address listed on the title page.

[18] An amalgamation of "Abloy" and "annihilator". Plus it sounds a bit like "Abloy" too.
[19] But unlike others, it actually works.

Conclusions

The Abloy Classic is an exquisitely designed lock. It has passed the most important test, the test of time. Exploits for this lock have been few and far between down the years. The discovery that The Problem 50 Paradox is not quite what it seems marks the difference between a mythically unpickable lock and the reality of the situation, which is that this lock (just like every other lock on the planet), is not invincible.

In some ways it is sad to witness the fallibility of such a security stalwart. But unfortunately, nothing can last forever and this is the only way security gets driven forwards.

The Abloy Classic can still be considered a *very* good lock and those who have the skills/tools to pick this lock are very few and far between. In reality, it is incredibly unlikely that any given Abloy Classic lock, in the field, will be picked. However, previous claims of "virtually pickproof" now clearly have to be revised. It is not just theoretically pickable but a practical reality.

Please note that this treatise does not encompass the author's entire oeuvre in relation to Abloy Classic. There are other more expedient attacks that will remain, for now at least, unpublished.

Also, this paper is not supposed to address the Abloy High Profile series of locks, which are similar in many ways but with enough notable differences to warrant their own examination.

