Beating the BiLock

www.lockpickingforensics.com
by datagram & Jon King, June 2010 – January 2011

This article discusses the history and operating principles of the BiLock pin-based sidebar lock series. We'll look at different generations of the lock and the various security features they offer. Finally, we'll review how BiLock stands up to various types of attacks, particularly lockpicking, decoding, and key simulation.

The BiLock is often cited as one of the most secure mechanical locks available, with proponents and marketing literature claiming the lock to be bump-proof and pick-proof. In this article we are publicly disclosing several design vulnerabilities that affect current versions of BiLock cylinders. These vulnerabilities range in severity with the most serious being covert decoding and destructive techniques. The tools and techniques presented in this paper are easily replicated. We encourage motivated readers to experiment and improve upon them freely.

All vulnerabilities were reported to BiLock North America and The Australian Lock Company several months before this article was published. On July 16th, 2010 BiLock North America published the following on their website:

> *"After extensive internal testing, and some additional upgrades, we are getting ready to submit an even more improved version for US and Canada certification. This BiLock system will far exceed the requirements set forth in UL 437. The new design will also thwart even the most sophisticated picking and decoding tools that are in use by the US intelligence agencies.*
>
> *We expect to be in full production of this newer generation product by the end of this year."*

This redesign is not a direct result of our research but luckily it coincided with our disclosure. We worked with BiLock during this time to get some issues addressed and we look forward to the revamped BiLock design in the coming months. Some details of the new design are included in the conclusion of this article.

The authors can be contacted at datagram.locks@gmail.com and jkthecjer@gmail.com. Additional articles and contact information are available at LockpickingForensics.com. Corrections, additions, comments, and criticism are all welcome. A list of references and additional resources is available at the end of this article.

1. BiLock First Generation

The BiLock is a series of Australian high-security locks originally invented by Brian Preddey in 1981. BiLock cylinders are produced and distributed by The Australian Lock Company and BiLock North America. BiLock cylinders are primarily marketed to institutions and the government, but after the media attention on key bumping their marketing shifted to include home owners and small businesses. From BiLock North America's website:

"*BiLock is an internationally acclaimed high security locking system in use by government, university, and hospital facilities who demand the very best. It is used by almost every major casino to protect their assets. It is also available for the homeowner who does not want to compromise the security of their family.*"

Patented in 1981, the original design is referred to as the BiLock First Generation (FG) and features twelve pins arranged in two rows of six (Figure 1.1). Two sidebars are placed at 3 and 9 o'clock in the plug, each interfacing with one row of pins. Unlike traditional pin-tumbler locks, the FG uses no driver pins. Instead, each chamber has a single spring-biased pin with holes on one side that interact with the sidebars legs (Figure 1.4). When all pins are properly positioned their holes line up with the legs of the sidebar, allowing the sidebar to retract and the plug to rotate.

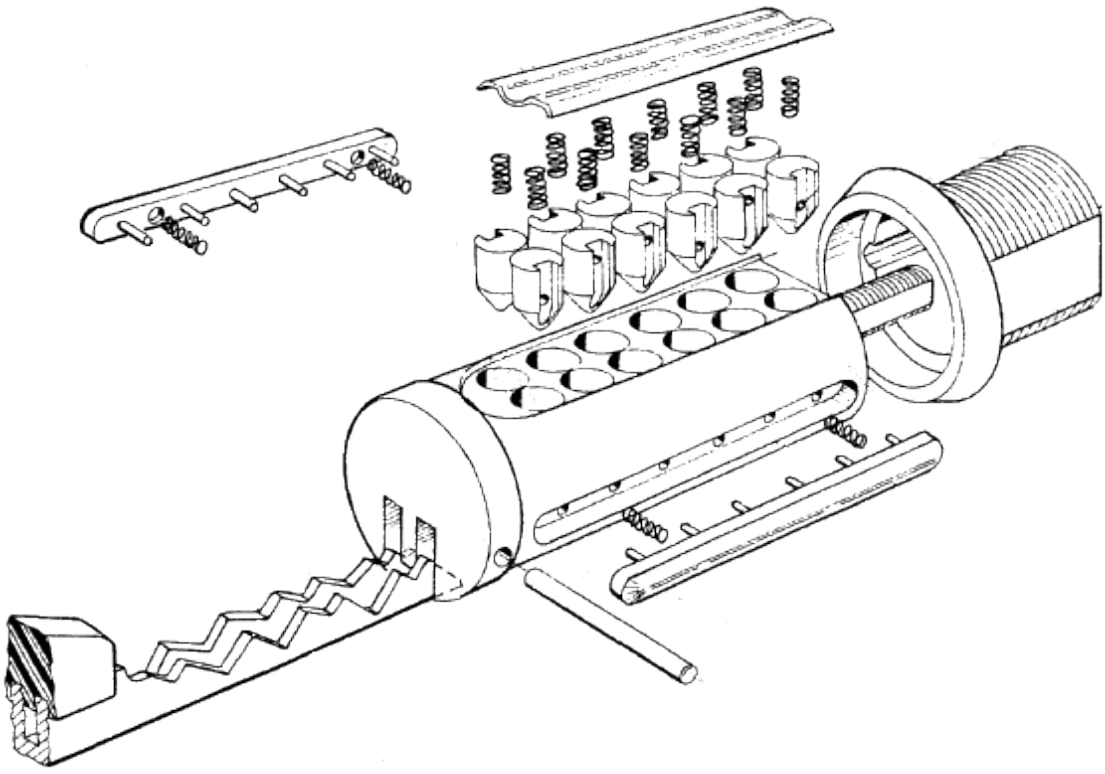
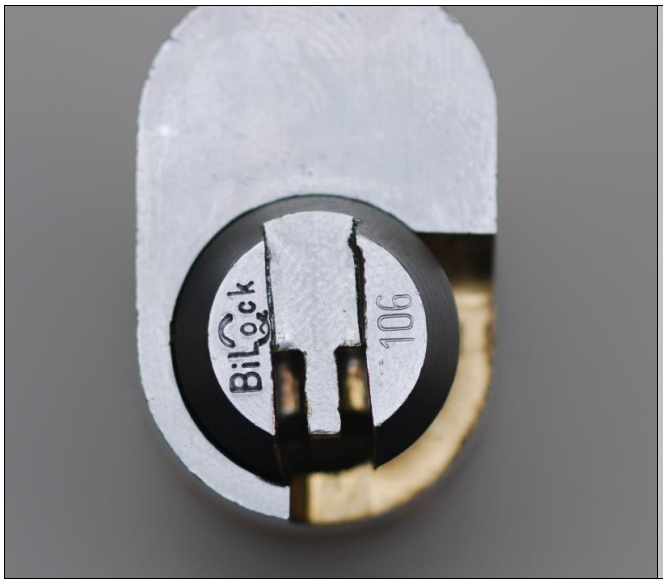
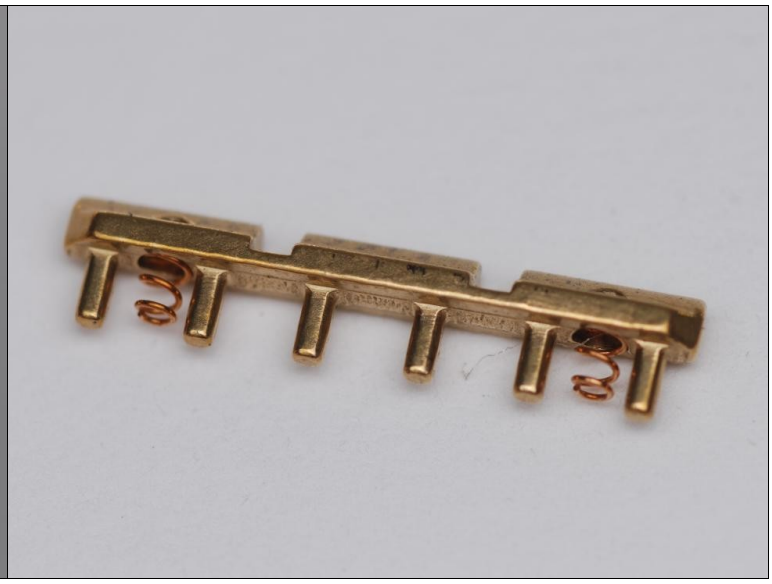
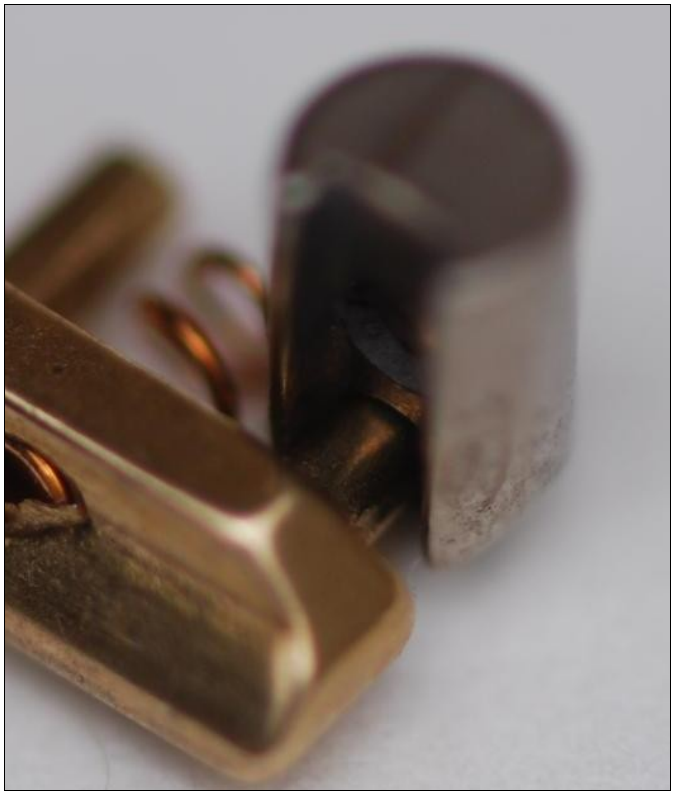


Figure 1.1: Cylinder design from the BiLock First Generation patent (US 4,478,061)





Figures 1.2-1.6: (Clockwise from top left)
(1.2) The BiLock FG with 106 keyway;
(1.3) the sidebar and sidebar legs;
(1.4) interaction between sidebar and pins;
(1.5-6) an empty/assembled (top) BiLock plug.



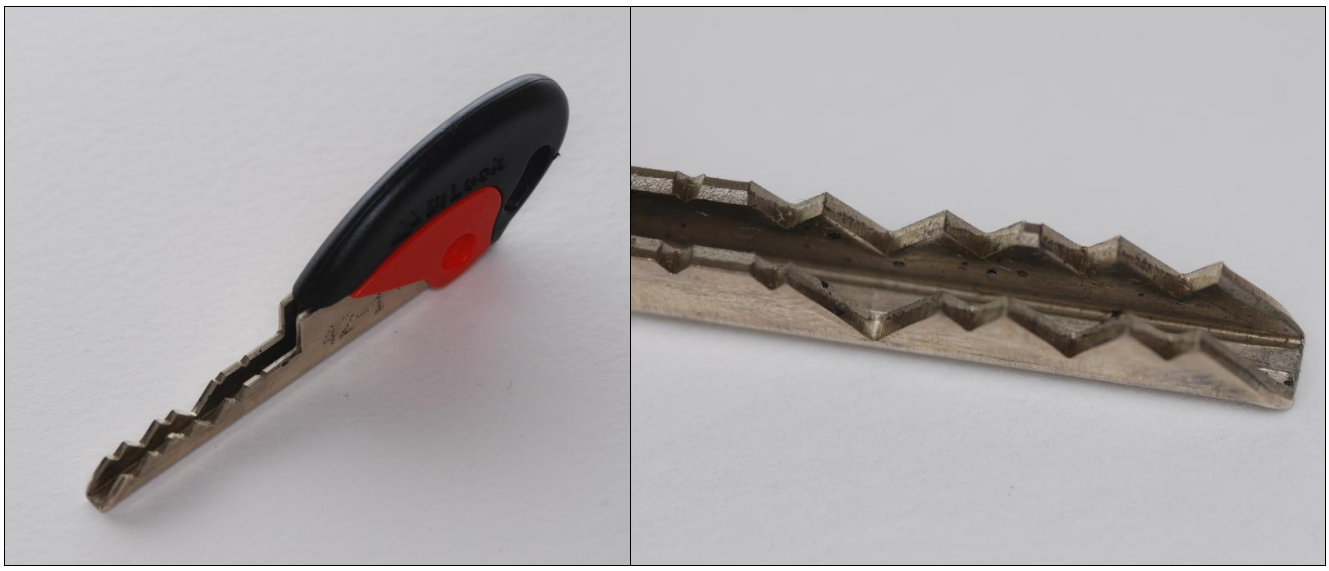


Figure 1.7: A BiLock key (left) and close-up of the double bitting; 102 profile (right).

One of the most unique parts about the BiLock is the use of a folded key (Figure 1.7). Made of nickel silver, the keys are constructed by folding a piece of metal to create the unique U shape. The key begins as a piece of metal folded in a “V” shape. A special key machine applies cuts to each side of the V and then the key is folded together and the bow applied. BiLock considers their key construction method to have various security benefits. We'll discuss the security aspects of BiLock keys in Section 4, *Security Analysis*.

The standard keyway profiles used are the 101 and 102. The warding pattern is difficult to see without examining the key, but most BiLock cylinders have the keyway number stamped directly on the plug (Figure 1.2). The 102 is the standard keyway profile but it contains no warding. The FG patent shows aggressive key warding which, to our knowledge, is uncommon in the field (Figure 1.8).

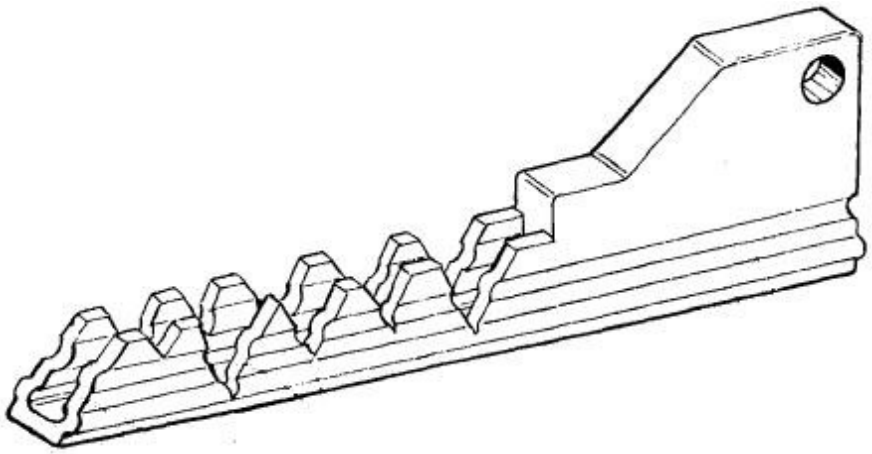


Figure 1.8: Key warding example from the BiLock First Generation patent (US 4,478,061)

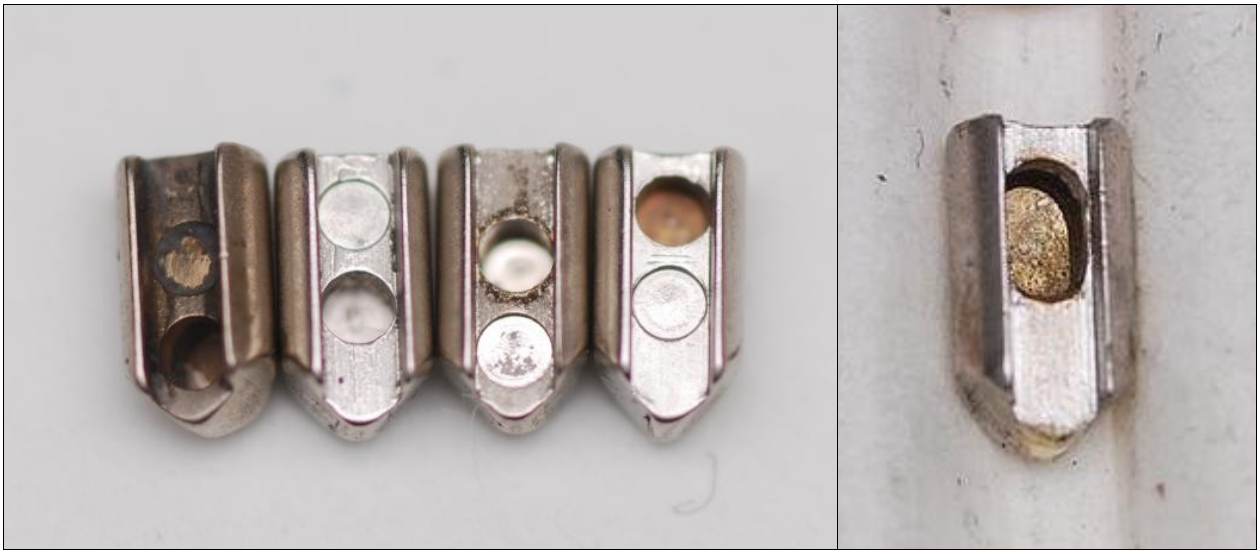


Figure 1.9: The 1-4 depth standard pins (left) and a 3+4 depth extended hole master pin (right).

The BiLock uses four pin depths and a total of fifteen available pins (Figure 1.9); the other eleven pins are for master keying. The BiLock allows master keying in the form of multiple true gates on each pin or extended true gates, such as a 3 and 4 depth combined (Figure 1.9, right).

Key bitting is coded 1-4, with 4 being the deepest cut on the blade. Pin coding is also 1-4, with 4 being the pin with the highest true gate. Master keyed pins have designations from A to K, with K being a 1-4 extended gate pin; it accepts all key cuts. A higher true gate position on the pin corresponds to a lower cut (but higher bitting number) on the key blade. Pinning and bitting codes are a combination of all key cuts, such as 241321-431124 for a key and A413I1-323B14 for a cylinder. A full pin and bitting reference chart is available in *Appendix A*.

The four non-master keyed pins are the only pins that have false gates. False gates are always at the +2 or -2 true gate position, depending on the depth. Older model FG cylinders may also use pins with smaller diameter false gates. Pinning a lock to include as many false gates as possible is a necessary defense against lockpicking. The high number of pins and the ease with which pins can be false set makes them surprisingly effective. With that in mind, only the 1 and 2 pins provide strong resistance; 3 and 4 engage the true gate before the false gate unless the pin is substantially over-lifted. We'll discuss lockpicking attacks against the BiLock in depth in Section 4, *Security Analysis*.

With four depths and twelve pins the BiLock has 16,777,216 theoretical key differs (4^{12}). BiLock cylinders have no MACS and the only keying restriction is that two #4 cuts (the deepest key depth) cannot be across from one another. This exists to prevent the key from bending or breaking at the low point. With this restriction in mind, there are just over 11 million available key differs. With each pin depth being available in eight pins (one normal and seven master) the BiLock offers extensive master keying possibilities.

Figure 1.10 (Left)**:** Serial number stamped on the plug.
Figure 1.11 (Right): Original BiLock FG key bow.

The plug has a serial number stamped on either the left or right side to frustrate replacing the plug after a destructive attack, such as drilling (Figure 1.10). Additionally, hardened inserts can be placed at various points to frustrate drilling the lock. The most common spot is the middle of the plug to protect both rows of pins.

More advanced security features are available for high security installations. One of the most interesting is a “staggered” pin version of the BiLock plug. In this design the pin chambers are not symmetrical, but instead one side is slightly offset. Of course, this style of plug requires keys that are also cut with their bitting offset. Unfortunately, the details of many other features are not made public. If you have any information on these features please contact us.

Modern FG cylinders use the same plug design as the BiLock NG (discussed next), but without the NG components installed. The keys now use the modern bow style, as well, but they do not include the NG's moving element. Older FG keys and cylinders can be identified by a blocky, lightly sloped bow (Figure 1.11) and a keyway profile with squared corners (Figure 1.2).

2. BiLock New Generation

In 1998, the BiLock New Generation (NG) was released. The NG is an extension of the FG design that includes a moving element in the key and a sidebar blocking rod in the plug. A casual observation of the lock reveals no major differences, but examination of the key reveals a small moving component inserted into the bow of the key. (Figure 2.1)

When the key is inserted, the face of the plug pushes and rotates the key component into position (Figure 2.2). This moves the sidebar blocking rod, allowing the sidebar to retract.

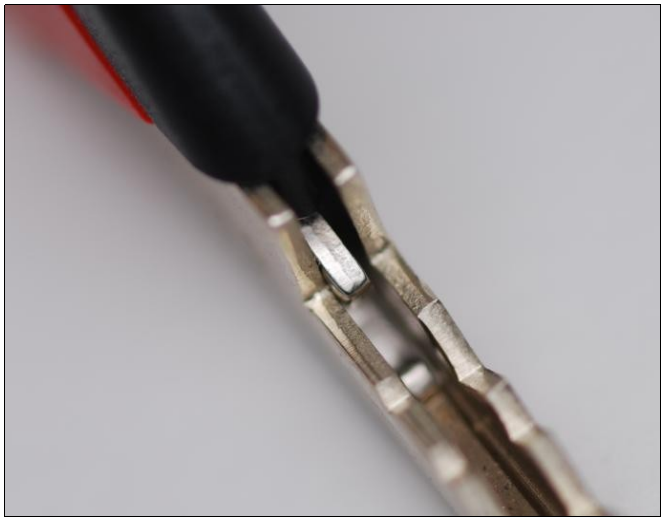


Figure 2.1: The NG key's moving element.

The main benefit of the NG's moving element is to prevent casual key duplication via casting a copy of a working key. It does not offer a significant amount of *additional* lockpicking resistance; it is simply picked when it binds. The patent version of the NG component includes a “barbell” version which blocks both sidebars. We assume this was not used in production because it will always bind first.

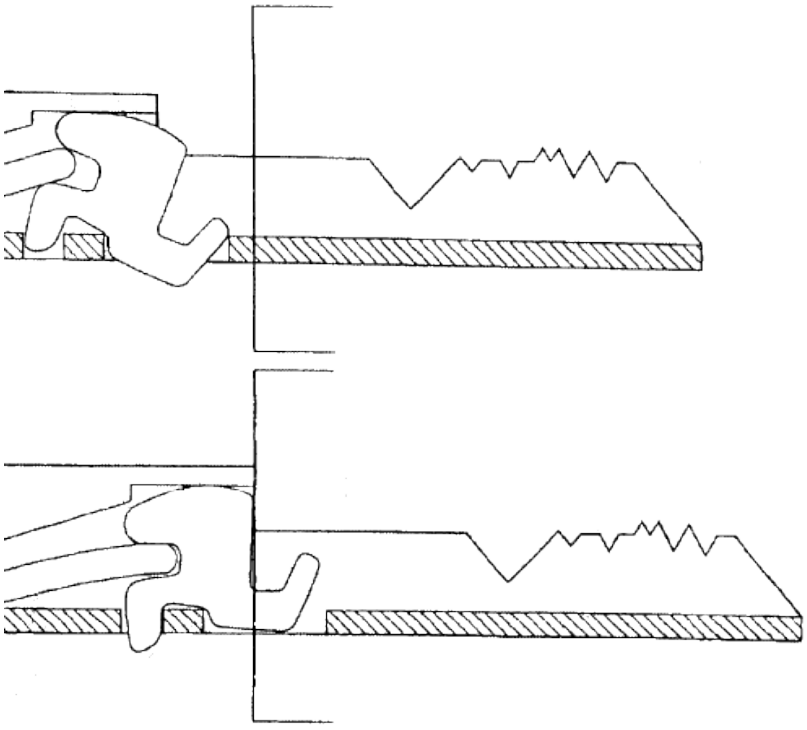


Figure 2.2: The key's NG component is rotated into position by the plug face. (US 6,681,609)

Figure 2.3: The plug's two NG components (left) and the key's moving element (right).

The NG system consists of components in the key and the plug. (Figure 2.3) The key component is simply a piece of nickel silver inserted between the fold of the key blade near the bow. The key bow keeps the key component in place by having a small plastic lip which rotates it to the default position. When the key is inserted into the lock, the plug pushes against and rotates this component so that it raises the NG pin in the face of the plug, moving the blocking bar up and out of the way of the three o'clock sidebar (Figures 2.4, 2.5). The plug component is spring biased downward to keep the sidebar blocked by default. The spring is held in place by the tip of the pin chamber casing used for the rest of the pins. The pin and blocking bar are held in place by the profile plate on the front on the plug. NG profile plates have milling to accommodate these components, and modern FG systems use the same plug design.

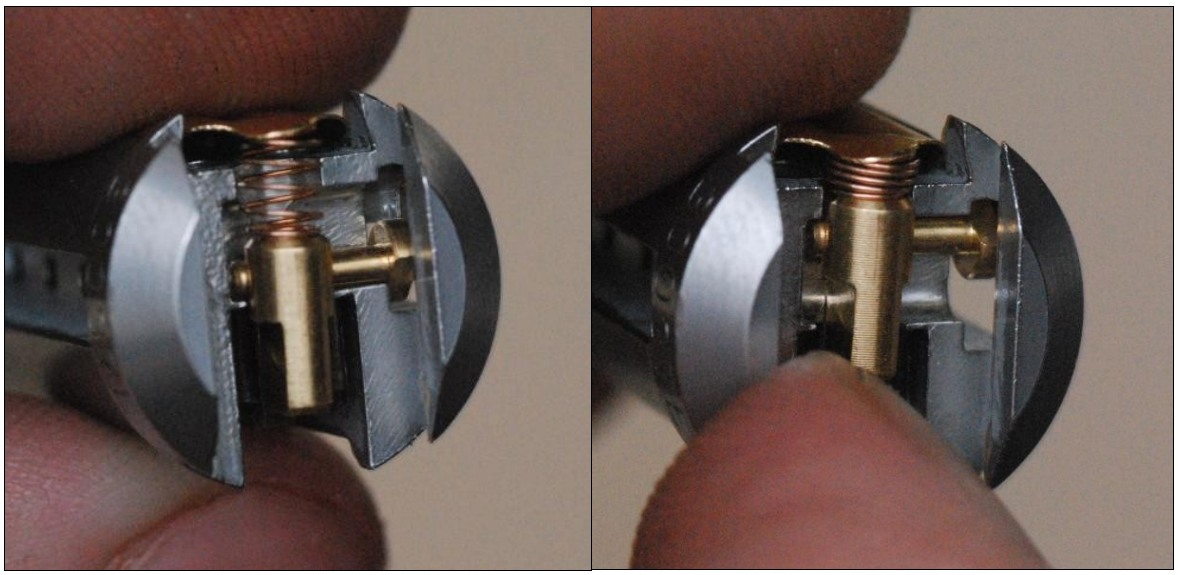


Figure 2.4: The plug's NG component is moved to free the right hand sidebar.

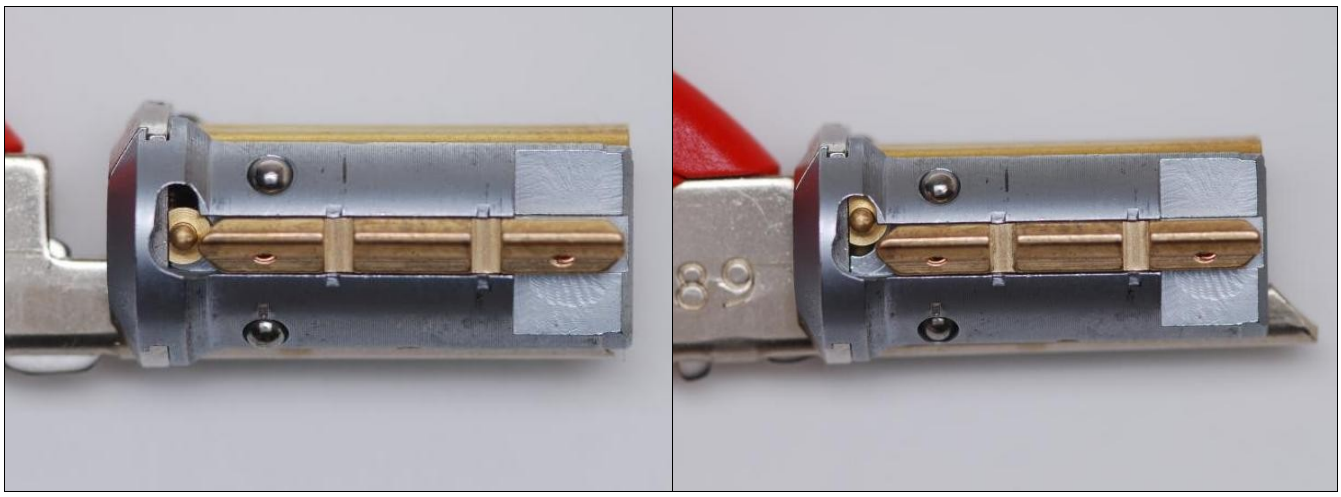


Figure 2.5: The moving element in the lowered (left) and raised positions.
(Rotation of the key component is also visible.)

The NG moving element draws many comparisons to similar systems, particularly the Mul-T-Lock Interactive and the Medeco m^3. In the Interactive, a moving component is placed in the first or second bitting position on the key. When fully inserted into the lock a component in the plug raises the moving element higher than the normal key bitting will allow, properly positioning one of the telescoping pin stacks in the lock. The Interactive is flexible enough to allow for three different types of moving elements (based on the pinning of the Interactive chamber) as well as variable position of the component in the plug. The m^3 contains a spring biased slider that blocks the sidebar from retracting until it is pushed out of the way. Sound familiar? The NG and the m^3 are similar systems, but both suffer from the same problem of being easy to defeat and difficult to improve.

The BiLock NG component is intended to prevent *casual* duplication of the key. This is not easily improved without heavily modifying the design of the moving elements themselves. In particular, it is not possible to lift the component *too* high; an attacker can simply raise the component until the sidebar is cleared. This is easy to do with any small tools; bobby pins, paper clips, and lockpicks are well-suited for the job. With little room for error there is no reason that varied moving element heights would make a difference. The Interactive checks if the moving element is too low *or* too high (a function of the pin stack), but it is difficult to modify the BiLock's moving element to do the same.

The NG component does have advantages over similar designs, though. The Interactive, for example, reduces the available key differs by taking up a pin chamber (dropping that chamber from twenty to three differs). The m^3 component is just as easy to defeat as the NG; simply push it to the right spot. The m^3 required the keyway to be widened and allowed manipulation tools more movement. This change led to several attacks against the cam of the lock. The NG is one of the few moving key components that does not make a compromise in the original lock design to include the new feature.

Many other changes have been implemented in the NG design, most of which have been applied to newer model FG cylinders, as well. The standard keyway profile (102) reveals that the newer keyways are lightly rounded at the edges (Figure 2.6). The newer profile is backwards compatible with the FG design (Figure 1.2).

One of the most interesting changes is a removable profile plate on the face of the plug (Figure 2.7). This is now standard in both FG and NG designs and allows the profile of the lock to be quickly changed. The center post of the profile plate actually makes applying heavy tension via traditional tension tools difficult. Using too much tension can easily break the center post, which makes applying further tension more difficult.

The profile of the lock can be easily identified via the number stamped directly on the plate. Older versions of the BiLock FG include warding as a fixed part of the plug and have the profile number stamped on the face of the plug.

Figure 2.6 (Left): Modern 102 profile; compare with the FG keyway in Figure 1.2
Figure 2.7 (Right): Removable profile plates and NG component milling.

3. BiLock Quick Change Core (QC/QCC)

The BiLock QC is a modified cylinder design that allows the cylinder to be rapidly extracted and replaced (Figure 3.1). Both the FG and NG designs are compatible with the QC system.

In the QC, the plug is not held in the cylinder by the cam, instead it is modified to use four ball bearings arranged radially around the plug at 2, 5, 7, and 10 o'clock. The top ball bearings (2 and 10 o'clock) are static and prevent the plug from being casually removed from the cylinder. The bottom bearings are movable and support the core removal function.

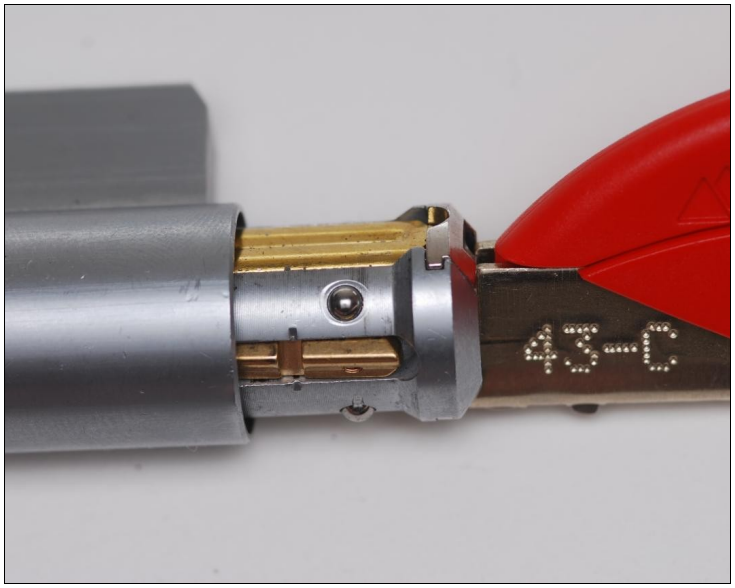


Figure 3.1: The BiLock QC core being extracted.

When the plug is rotated 45º in either direction the top ball bearings line up with slots in the cylinder (Figure 3.2). If a control key is inserted the plug can be removed by pulling on the key. A control key is just a working key with dimples by the first bitting cut (Figure 3.4). When the key is pulled the bottom ball bearings fall into the dimples on either side of the key and allow the plug to be removed. Once removed, a new core can easily be installed by simply inserting it (requires a control key) and rotating it back to the normal position.

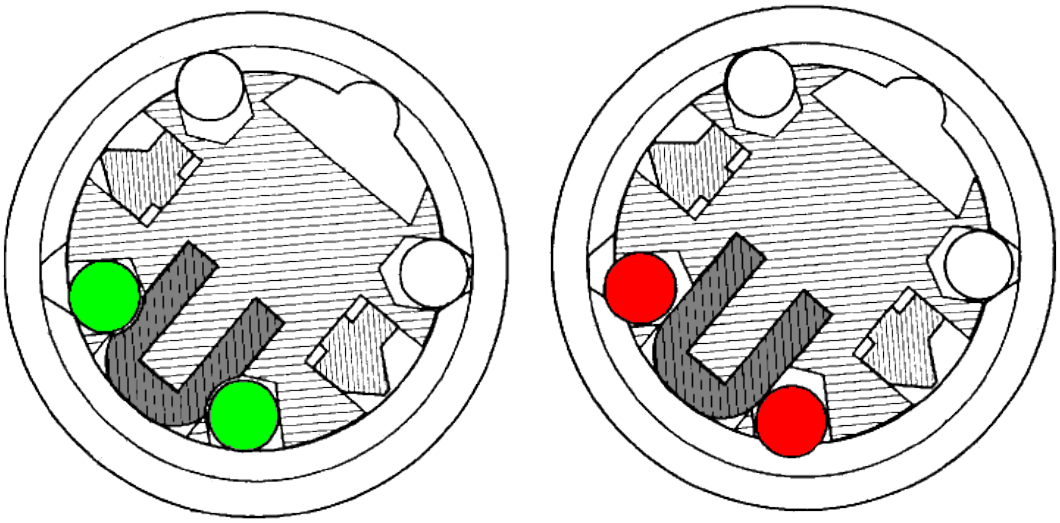


Figure 3.2: Control key (colored) and retainer bearings (white) in the plug. (US 6,076,386)

Figure 3.3: Control key bearings in the locked (left) and unlocked (right) positions.

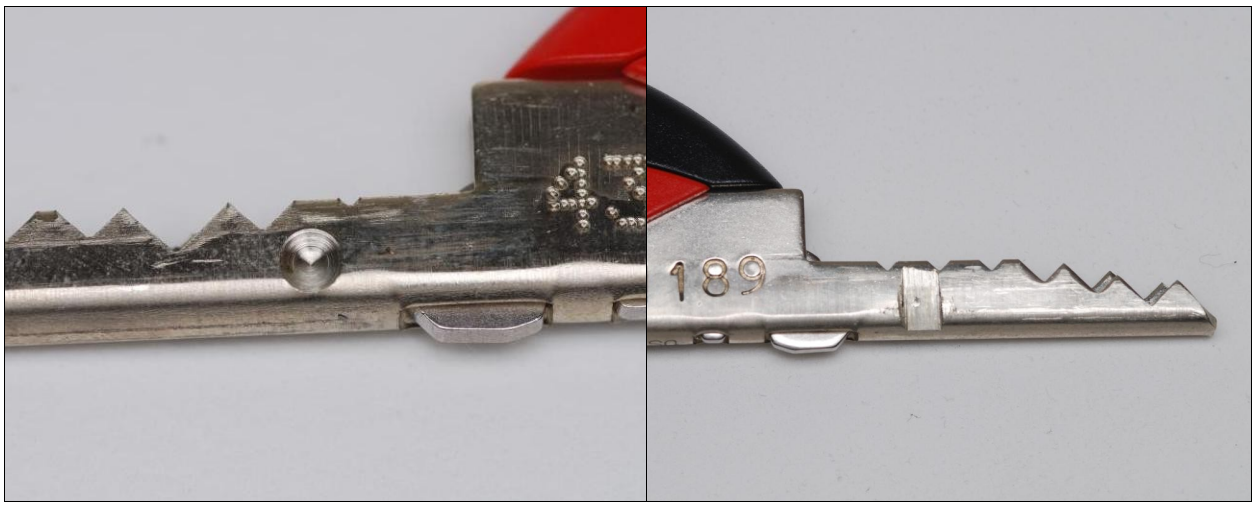


Figure 3.4: A QC control key (left) and modified user key (right) that can remove cores.

One shortcoming is that any user key can be modified into a control key by removing material where the control dimples should be (Figure 3.4, right). Control keys can be identified by the dimple on their key bitting and are (usually) marked XX-C, such as “43-C” in Figure 3.1.

The QC plug requires the cam to be affixed to the cylinder itself, held in place by a spring clip. Only the top two ball bearings retain the plug from being removed; the other two are free-floating and only restrict core removal when a user key is presented. This method of plug retention is a tempting target for destructive entry techniques.

4. Security Analysis

The strength of a lock is measured by both advantages and shortcomings. As consumers we look for locks that protect against common vulnerabilities but understand that no lock can be secure against every possible attack. Lockpicking and key bumping receive the most media attention but they aren't the only way locks are attacked. Too often we look for a solution to the current threat rather than consider the variety of ways in which a lock can be defeated. In this section we'll analyze how BiLock designs defend against a variety of threats.

We are not making any claims about the security of the BiLock or the implications any of these vulnerabilities have on real-world installations. Instead, we will present what we have found and leave any conclusions about the security of the lock to the reader. Remember that the security of a lock heavily depends on context, particularly the security requirements of a given installation.

Key Control

Key control refers to the ability to prevent attackers from obtaining, duplicating, and simulating both blank and working keys for a lock. This is important in a high security lock because it is generally easier to attack the key rather than manipulate the lock. The BiLock bases its key control on a variety of factors.

First is the limited ability for attackers to obtain key blanks. This is certainly true; only dealers can obtain them from BiLock, and they are not commonly available on the Internet. Second, keys should not be easy to duplicate or simulate. Duplication refers to taking a working key and a blank key and being able to copy the bitting pattern from the working key to the blank. Preventing duplication is a matter of controlling the availability of key blanks and, where possible, complicating the process of accurately copying cuts from one key to another without using a key machine. Simulation refers to the ability to use something other than a key blank to properly position each component. Simulated keys are traditionally flat pieces of metal, usually steel shims, that are thin enough to fit between the keyway warding and cut to position components in the same was as a normal key. Key simulation is combated with aggressive keyway warding, moving key elements, and bitting cuts that are difficult to simulate.

BiLock keys of all generations are difficult to duplicate given the limited availability of blanks. Blanks also come unfolded (bent at 90˚), so you would need to be able to cut the key as well as fold it properly. On the other hand, BiLock keys are relatively easy to simulate given the lax keyway warding used in many systems, especially the standard 102 profile. It's a relatively easy process to create a simulated key out of any small shim, a credit card, or other similar materials (Figure 4.1). Of course, this process requires that you are able to visually decode a key, measure a working key's bitting, or decode the pins from a disassembled lock.

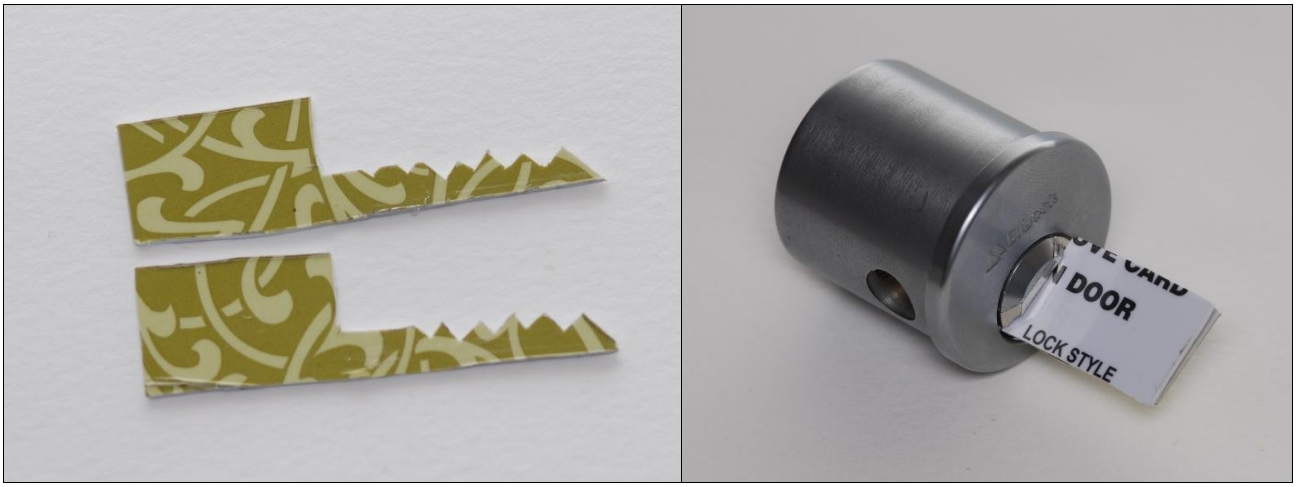


Figure 4.1: BiLock keys made out of magnetic stripe cards opening a BiLock rim cylinder.

One of the main assumptions about the BiLock is that you need to simulate the folded key itself. This is not true; you can make independent blades instead. Doing so also keeps the center of the keyway free, allowing you to position the NG component manually.

The intent of the NG is to protect against molding and casting a copy of a working key. A side effect of the design is that the newer NG keys are also patent protected, reinforcing the limited availability of NG blanks. Despite this, FG and NG keys can be molded and cast to duplicate their bitting. While traditional "clam" impressioning kits that use clay molds are unsuitable for BiLock keys, a silicone based mold will be able to perform a full 3D cast of the key, including any warding and core removal dimples. A cast NG key can be modified to include a hole where a wire can be inserted to properly set the NG component by hand (Figure 4.2).

Figure 4.2: A BiLock NG key molded with silicone and cast using urethane.

The last thing we'd like to discuss concerning key control is the ability to turn a user key into a core removal key in a QC system. The ability to remove a QC core with a user key might seem innocent; don't we already have the bitting if we have the key? Consider the implications in a master keyed core; removing the core allows disassembly and decoding of the pins. In turn, this lets us escalate our privileges and potentially compromise the whole master key system. This is complicated by the limited availability of key blanks but we can use credit card keys to make ourselves master keys, as shown earlier.

Lockpicking

The BiLock is highly resistant to traditional lockpicking attacks but we hesitate to say that it is “pick proof” as their advertising claims. We believe a sufficiently skilled and motivated attacker is capable of picking a BiLock cylinder, though it does take a considerable amount of practice and skill. From BiLock North America's website:

“There are claims of people picking a BiLock cylinder. In every case we have researched, the operating key was already in their hand and they refused to let us examine the actual lock. This leads us to believe that the locks were "modified" to make it look easy to pick. The locks manufactured by BiLock are to the highest standards and quality. We have yet to personally witness any original BiLock cylinder being picked open without a key.”

Presumably, this is in response to a large number of videos online which show people picking BiLock cylinders. We feel it is unfair to claim that all these videos are without merit, but we cannot comment on their validity. The statement about having an operating key brings up a good point. Is the security of a lock against lockpicking a matter of key control? Does having information about the bitting of the key discount the ability to manipulate the cylinder? In our opinion, resistance to lockpicking must be a combination of the two. While having partial or full information about the key bitting allows you to pick the lock with less guesswork, it still requires a considerable amount of skill to manipulate components to their opening position. We also feel that lockpicking is a less attractive attack when bitting information can be obtained, especially considering how readily working keys can be simulated.

Traditional over-lifting of modern BiLock cylinders is not possible. In this context, overlifting refers to the act of making a “comb” pick to physically lift all pins above the sidebar legs. This does not quite work but can be modified to use excessive force to lift the pins above the sidebar legs. In our tests a wedge tool can be used to forcibly over-lift the pins, but it is a destructive attack in every sense of the word.

Another form of over-lifting involves raising all pins, applying tension, and then letting pins drop down to the shear-line (in this case, dropping so that their true gates grab onto the sidebar legs). This attack has limited effectiveness against the BiLock because of the position and effectiveness of false gates. This may be more effective in master-keyed systems depending on the bitting of a given lock.

Key bumping

The lack of driver pins makes the BiLock bump-proof. There is not much more to be said about this, though “bump proof” is one of BiLock North America's main marketing points.

Impressioning

We have not been able to fully explore impressioning attacks against the BiLock at this time. What follows is a brief discussion of the theory of impressioning the BiLock and what pitfalls an attacker may discover.

One of the problems with impressioning the BiLock is the assumption that a single blade must be presented. Obtaining or creating folded keys is difficult but it is theoretically possible to impression the lock using independent blades. The difficulty with this approach is situating and maneuvering each blade without generating false readings. On top of this, applying torsion with either approach is difficult. In normal impressioning attacks the blank key is used to provide tension, but the design of the BiLock key makes it relatively weak when extreme torsion is applied, especially if there is a deep cut close to the bow.

The impressioning process itself is complicated by the dynamics of how key cuts, sidebar legs, and the gates pins interact. The main concern is that the design of the pins and the cuts on the key offer some subtle problems to an impressioning attack. In particular, the pins rest on the sides of key cut rather than stopping at the tip of the pin, as it is with normal pin locks. Impressioning this lock would mean that the tips of pins make contact with the bitting cuts directly, potentially changing the exact depth of a given bitting. Additionally, when a sidebar leg pushes into a false gate it has a tendency to lift the pin so that the center of the false gate aligns with the sidebar leg, slightly lifting it away from the key. This could cause false readings, namely assuming that a pin is correctly set when it is in a false gate.

Though all of this seems daunting, the BiLock should theoretically be easy to impression once these obstacles are overcome: the lax warding in the majority of cylinders allows for a wide range of movement during impressioning; the low number of depths per component makes it relatively easy to cut each position once binding marks can be reliably obtained. Care should be taken to develop a new set of keying depths when filing a blank because the pins will not be resting on the slopes of the cuts as they are in a normally cut key.

At this time we have not successfully impressioned a BiLock cylinder and have not heard of anyone else doing so, either. There are many areas of impressioning, particularly the use of self-impressioning materials (such as foil), that have not been explored. If you have any information about this attack that you would like to share please contact us.

Decoding

Decoding is a somewhat ambiguous technique that allows an attacker to get the information needed to make a working key but does not necessarily produce a working key or an easy way to open the lock. Impressioning, for example, is an invasive decoding technique that allows an attacker to decode the bitting of a working key as well as open the lock. Another decoding technique is to simply look at someone's key and attempt to identify the bitting pattern. However, even with the bitting pattern it may be difficult to make a working key for that lock. Given the ease with which we can simulate BiLock keys, any decoding technique becomes a very powerful attack that can open a lock.

The design of the BiLock, particularly the lack of driver pins and the constant length of all pins, make some traditional decoding techniques unusable. Of course, all of the decoding techniques that attack the key work, namely measurement and visual decoding. The low number of depths make it easy to “sight read” keys, even from a moderate distance. Aside from this we want to know if there are any methods of decoding the lock without disassembly or obtaining the key. There are two methods to decode the lock covertly, one of which we consider a design flaw in the BiLock.

A cursory examination of the pin design reveals that the slots used to prevent the pins from rotating extend to the bottom of the pin (Figure 4.3). This allows a small wire to be injected into the channel to decode the position of the true gate on each pin (Figure 4.4).

Figure 4.3 (Left): The channels on each pin extend through the length of the pin.
Figure 4.4 (Right): A wire probe is injected in the channel to decode the true gate position.

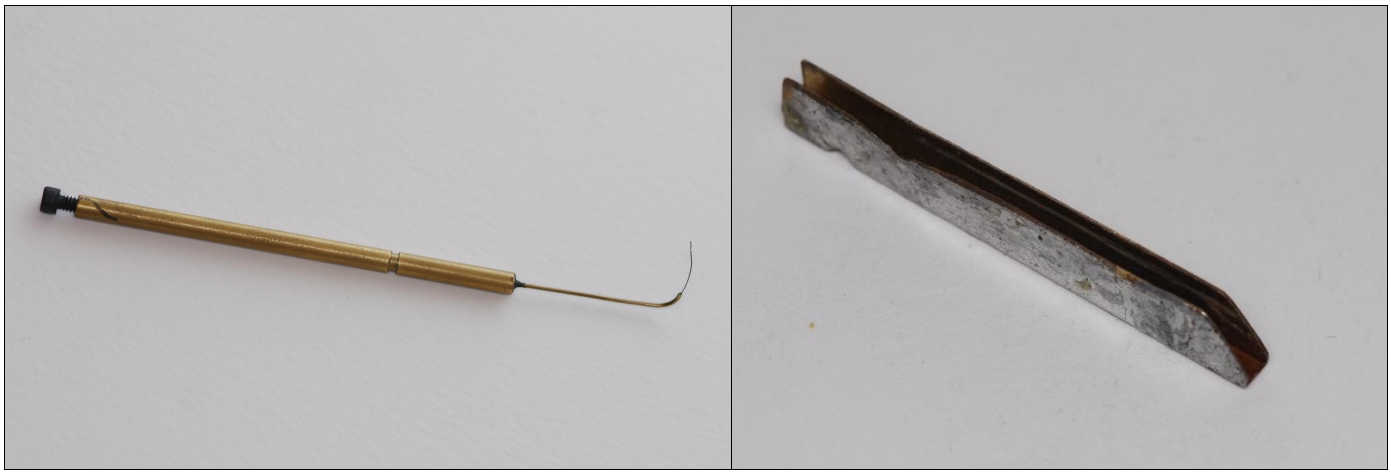


Figure 4.5 (Left): Our wire injector decoding tool
Figure 4.6 (Right): Lifting tool used to raise the pins.

We made a tool to probe the gates, a simple wire injector with a small scale along the shaft (Figure 4.5). It is inserted into the keyway under each pin. The wire travels up the pin's channel to probe the position of the true gate which can be decoded via the scale on the shaft. False gates can be identified by their poor ability to “grab” the wire and the feedback the tool gives as the wire scratches against the wall of the false gate (true gates are too deep for this). We have tested this tool with non-master keyed cylinders and assume that the process would be simplified for heavily master keyed cylinders due to the lack of false gates on master pins.

One problem we encountered was maneuvering the tool in the lock. At rest, all pins sit near the floor of the plug and make it difficult to move the wire into the channels. We made a lifting tool that would fit into the keyway around the center post. This tool has two functions. First, it moves all of the pins to the top of the keyway, giving us more room to move the tool. Second, it allows us to inject the wire into each channel without disturbing the lift of the pin. Without the lifting tool you'll inadvertently be raising a pin by moving the injector beneath it, making it difficult to get accurate readings. The lifting tool solves this problem by lifting all of the pins to the same height and letting us move around underneath them without disturbing their position.

Closing the gates on these channels stops this attack, but that may be difficult depending on the BiLock's manufacturing process. In particular, the assembly of the entire lock may be hindered by closing the channels. The sidebar prevents pins from rotating; it's logical the sidebars are inserted before the pins so that they are properly rotated. If the gates were closed this might not be possible; it might prevent the pins from falling into the pin chambers.

Replacing pins in existing locks is easier, but there is a problem for QC users. BiLock QC cores have their sidebars crimped in place to prevent them from falling out when the core is removed. QC cores cannot be disassembled easily to replace the vulnerable pins but the core itself can always be removed and replaced entirely. This might be expensive and time consuming endeavor depending on how many cylinders you want to re-pin or replace.

The second decoding method comes from Falle Securities, a well known covert entry tool manufacturer, who sells a government-level tool that can covertly decode BiLock cylinders and create simulated keys. This tool is extremely difficult to obtain; sale is restricted to government covert entry personnel and it is rather expensive. Little public information is available on the tool; when we began our work we could not find anything about the tool other than its existence. We provide a complete description of it here. Unfortunately, we are not able to provide any photos of the tool.

The Falle tool is a system of smaller tools, namely John Falle's variable key system and a set of pin-and-cam decoding instruments. The Falle tool can open both normal and offset BiLock cylinders. The first part of the tool is the variable key system; a set of simulated metal key blanks for the BiLock which have each bitting position scored on the side. Blanks are thin enough that they can be cut to code with a pair of scissors.

The simulated keys are loaded into a cradle which positions them properly in the keyway. The cradle itself connects to a large tension ring outside of the lock which includes a channel for the decoding probes to align on. Each decoding probe is more or less a lockpicking tool similar to a half diamond or deforest pick. It is inserted into the lock and tension is applied. Whenever a pin binds it will be detectable by the movement of the probe. The attacker marks down which pins are binding and cuts those key positions down. Eventually, pins are correctly positioned and no longer bind. When all pins are positioned properly the lock opens. In a sense, the Falle tool is an evolved impressioning attack that does away with the notion of requiring key blanks. With tension applied via the ring and not the key, heavy tension can be applied to the plug without worrying about the integrity of the simulated key.

These are the two main methods we have found to covertly decode BiLock cylinders. Luckily, the first can be stopped by denying access to the pin channels. The Falle method of decoding exploits a fundamental flaw in the design of the lock and cannot be easily defended against. Aggressive keyway warding may provide minor defense against both attacks, though. BiLock North America and the Australian Lock Company have told us newer BiLock designs should defend against our decoding method. A preview of the new design is available in the conclusion of this paper.

Destructive Entry

Unfortunately the design of the BiLock makes it vulnerable to a number of destructive attacks. Many of these attacks can be performed rapidly with common hands tools by a low skill attacker. We have not considered certain factors, such as noise, in evaluating the severity of these attacks. *Due to the sensitive nature of destructive attacks this section will contain limited vulnerability information*. This section is by no means exhaustive; we don't have an unlimited supply of cylinders to destroy!

The major concerns for the BiLock are that the design of the center post which separates the pins is relatively weak compared to the rest of the lock, and the brass used for many components, specifically the sidebar, is not strong enough to prevent certain attacks.

Older models of the BiLock have issues with being torqued open due to the short distance each sidebar must travel to allow the plug to rotate. Applying extreme torque causes the sidebars legs to push into the pins, compacting them and slightly tilting the sidebars vertically. In older locks, this can be enough to allow the sidebars to retract.

The design of QC cylinders makes them especially vulnerable to drilling attacks. With the plug retained only by the ball bearings on the top of the plug (see Figure 3.2), the plug can be removed by drilling the plug and cylinder at these two points. Drilling of the pins themselves is also possible, as is drilling out the center post to remove all the pins. The standard BiLock cylinders sold in the United States do not include any anti-drilling mechanisms, but they are available to higher end or customized installations. We are not aware of any QC design that shields the retaining ball bearings, however.

One attack we discovered exploits a fundamental flaw in the way that sidebar legs and pins interact. When a sidebar leg enters a true or false gate the pin is immobilized if tension is applied. If strong vertical force is applied to the pin it is possible to shear the sidebar legs (Figure 4.7). Once all the legs are sheared any key will work to open the lock.

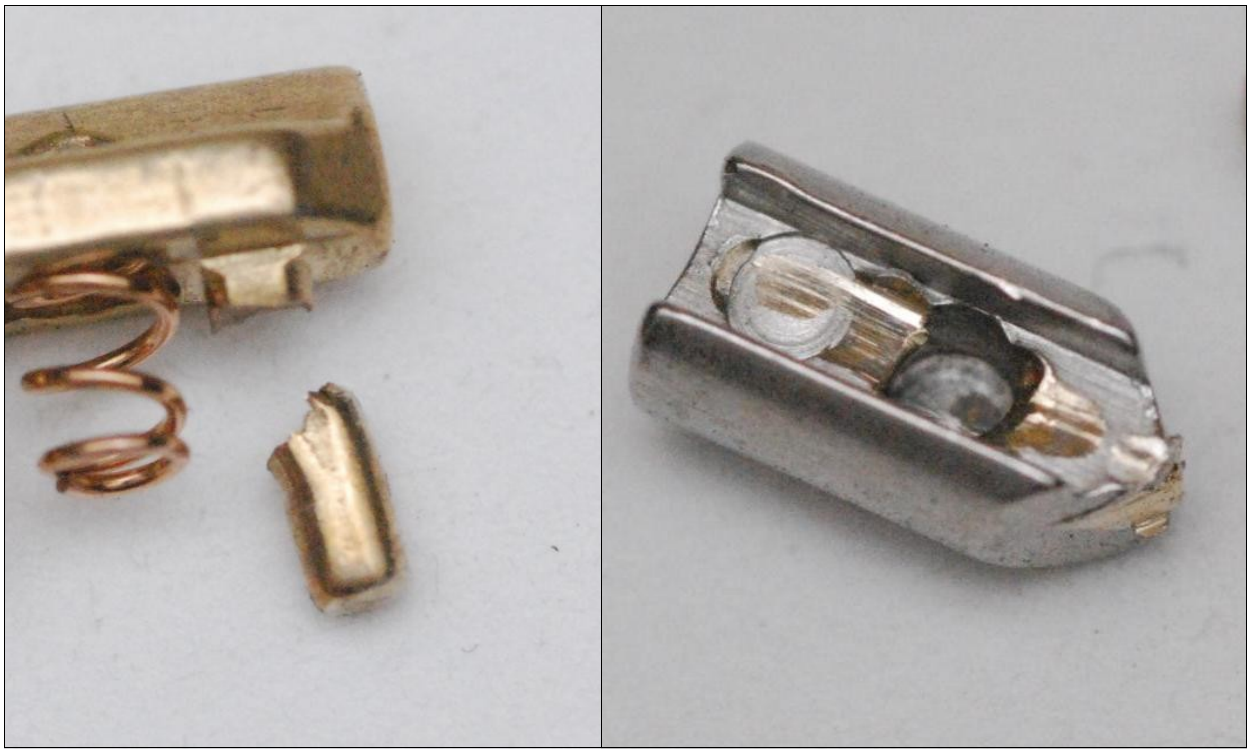


Figure 4.7 (Left): Sidebar legs can be sheared via torque and vertical movement of the pins.
Figure 4.8 (Right): Forensic evidence of the leg shearing attack on the pins.

When torque is applied the pins will bind in the same way that they do during lockpicking. When raised, the binding pin's true or false gate will *eventually* engage the sidebar leg. If sufficient vertical force is applied, it will not matter which gate engages first, as the force will literally tear through the material between the true and false gates until it reaches the true gate, at which point the pin has enough grip on the sidebar leg to fully shear it (Figure 4.8).

At present this attack is time consuming due to having to individually shear sidebar legs. In theory, this attack could be done in one fell swoop if all sidebar legs with held in place by a true or false gate at the same time. We have not fully explored this area of attack but we feel that it has the most promise in terms of rapid destructive entry. In the future we will be experimenting making our own hardened keys that be used to reduce the time necessary for entry with this attack.

One of BiLock North America's proposed defenses against our decoding method (and as an additional anti-picking measure) was to increase the depth of false gates, making it more difficult to distinguish between true and false gates. While this might be effective, we expressed concern over making the gates deeper because it makes this attack more effective by ensuring the false gates have a firm grip on the sidebar legs.

There are, of course, many other ways to destructively attack locks. Unfortunately, we are not able to test every possible method due to our limited resources. If you have any attacks that you feel we should include in this section please contact us.

5. Conclusion

As stated at the beginning of this paper, we worked with BiLock North America during their 2010 design process. This was not a result of our work, but instead coincided nicely with our disclosure to them. We made several suggestions for consideration in new or improved BiLock designs. A quick summary of our recommendations for improving the BiLock:

1. Use better materials for the sidebar.
2. Close the channels on the pins.
3. Place the keyway identifier on the back of the profile plate.
4. Provide more aggressive key warding in standard locks.

We were informed by BiLock North America that a new version of the lock will be submitted for UL 437 certification in the United States in 2011. This version should have defenses against some of the attacks mentioned in this paper, particularly defenses against our decoding method. BiLock North America provided an image of an early version of the new design that was submitted for European certification (Figure 5.1).

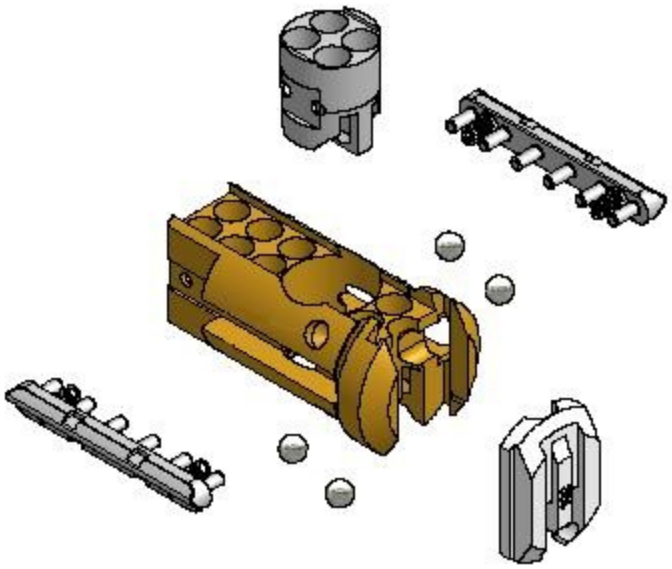


Figure 5.1: New BiLock design (QC) with steel sidebars and anti-drilling plug modification.

The main change in this design is the use of steel components for the sidebar and profile plate. This helps to prevent a number of destructive attacks and makes the BiLock a more durable lock overall. The large cylinder in the center of the plug is meant to be a defense against drilling of the pins. We think a further improvement to this design would be to place the QC ball bearings behind the steel cylinder to protect them from drilling as well.

The BiLock is a great lock design but has room for improvement. We've spent many months thinking about the BiLock but we're sure that there is more to discover. We encourage motivated readers to explore new ways to attack *and* improve the BiLock and any other locks that they are interested in. Please contact us if you find anything about the BiLock that you think we should include in this article.

We're happy to see many enhancements coming and to know that lock manufacturers are focused on improving their designs. We hope you enjoyed this article on the BiLock series of locks. Please keep reading for a list of resources that you might be interested in on locks, forensics, and physical security.

Sincerely,
datagram & Jon King
January 2011

Credits, Thanks

First and foremost we must thank Tom DiVito of BiLock North America for his assistance in the disclosure process with BiLock North America and The Australian Lock Company. Thanks Tom!

A big thanks to Tom Ballard for help and inspiration with key simulation. It was Tom's research that got us started and motivated us to continue our work. Locksport International was instrumental in helping us obtain BiLock cylinders to work with; a big thanks to them as well!

Many other people were also instrumental in helping prepare and review the article. In no particular order: Deviant Ollam, Doug Farre, Babak Javadi, stderr, Schuyler Towne. Barry Wels, scorche, Josh Hickenlooper, Squelchtone, viduata, Matt Block, sfi72, and all the fine folks at Security Snobs.

Resources

Lockpicking Forensics – lockpickingforensics.com

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

LockWiki – lockwiki.com

A collaborative online encyclopedia that focuses on locks, safes, and physical security. Feel free to help out and contribute! Lockwiki's Community Portal also lists many locksport groups and related sites that you might be interested in. Most of the photos used in this article are available under Creative Commons licensing at Lockwiki, as well.

The Amazing King – theamazingking.com

Jon King's personal website. Information about lock and physical security research, locksport, computer programming, cryptography, and cryptanalysis. Details on Jon's Medecoder, a Medeco decoding and picking tool, are available at his site.

Patent References

US 4,478,061	BiLock FG cylinder	(1982)
US 6,076,386	BiLock QC cylinder	(1998)
US 6,681,609	BiLock NG cylinder	(2001)

Appendix A
Key System Specifications

The following is a reference for BiLock pin and keying specifications. These numbers apply to all standard First and New generation BiLock cylinders, both EX and QC cylinder formats.

Pin	True gate(s)	False gate
1	1	3
2	2	4
3	3	1
4	4	2
A	1, 2	-
B	1, 3	-
C	1, 4	-
D	2, 3	-
E	2, 4	-
F	3, 4	-
G	1, 2, 3	-
H	1, 2, 4	-
I	1, 3, 4	-
J	2, 3, 4	-
K	1, 2, 3, 4	-