Security Vulnerability Report: BEST® Interchangeable Core (IC) Lock System

Gabriel Marie Lavoie St-Gelais

November 17, 2025

Abstract

This document provides an overview of a security vulnerability identified in the BEST® Interchangeable Core (IC) Lock System. The objective of this report is to disclose this vulnerability and demonstrate how easily it can be exploited, in order to encourage improvements in security measures.

1 Introduction to Interchangeable Core (IC) Systems

1.1 What is an Interchangeable Core (IC) System?

An Interchangeable Core (IC) lock system is a type of lock where the core, or inner locking mechanism, can be removed and replaced without dismantling the entire lock assembly. IC cores are commonly used in commercial, institutional, and government settings, where security needs may frequently change, and the flexibility of rekeying quickly is crucial.

1.2 How IC Core Systems Work

IC cores use a system of control and master keys to manage access:

- **Control Key**: The control key is a specialized key that allows authorized individuals to remove and replace the core of the lock. With a control key, the IC core can be removed and swapped out, enabling quick rekeying without replacing the entire lock.
- **Master Key**: In many IC core systems, a master key grants access to multiple locks, offering flexibility for different levels of access within a facility. This is especially useful in buildings where a single person, such as a manager or security personnel, may need access to many areas without carrying multiple keys.

IC core systems provide convenience and cost savings by allowing easy rekeying without the need for lock replacement, making them a popular choice in high-security environments.

1.3 Why Investigate Security Vulnerabilities?

The primary motivation for investigating security vulnerabilities in systems like the IC core is to improve overall security. By understanding potential weaknesses, manufacturers and users can address and fix them, strengthening the protection of assets and people.

People often question why breaking down a security system can lead to increased security. The logic is straightforward: by identifying weaknesses before malicious actors do, we can proactively protect against them. Testing and studying vulnerabilities can lead to valuable insights, resulting in stronger designs, improved lock standards, and more robust security solutions.

1.4 Purpose of This Report

This report serves to responsibly disclose a vulnerability found within the BEST® IC core system. The goal is to inform relevant stakeholders of potential security gaps while advocating for system improvements. By responsibly documenting this vulnerability, we aim to enhance awareness, encourage better design practices, and ultimately contribute to the security and safety of facilities relying on IC core systems.

2 Elements Required to Compromise the IC Core System

2.1 List of Materials and Tools Required

General Tools

- Hammer
- Caliper (for measuring pin lengths and key cut depths)
- File (for manual key cutting and finishing)
- Steel wool (for cleaning key edges)
- Anvil (for straightening bent keys) (optional)

Locksmith-Specific Tools

- Cut key / blank key
- Lishi cutter (for fast key cutting) (optional)

3D-Printed or Specialized Tools

- Decapping Block — holds the IC core during pin extraction
  (Commercial: $400, 3D-printed: $0.30)
- Pin Unloader or just a screwdriver that is small enough
- Pin Receiver — collects extracted parts
  (Commercial: $400, 3D-printed: $0.40)
- 3D-printed guide (for key shaping and cut alignment) (optional)

Documentation Tools

- Spreadsheet software (Excel or Google Sheets) (optional)

Consumables and Miscellaneous Materials

- Electrical tape (for the tape method when copying keys)
- Solder (for repairing over-filed keys) (optional)

2.2 Prerequisites

This document assumes that the reader has a foundational knowledge of locksmithing, specifically with BEST® IC core systems. The intended audience includes:

- Professional locksmiths familiar with installing and servicing BEST® IC cores.
- Intermediate lock-picking practitioners with or without knowledge of BEST® lock and IC cores.
- Individuals familiar with IC cores.

2.2.1 Key System Hierarchies (System)

A Key System Hierarchy organizes keys based on their access level. In a hierarchy, a **control key** has the highest level of access, enabling removal and replacement of lock cores. Next, **master keys** allow access to multiple locks within a subset of the system, and individual keys provide access to single locks only. This hierarchy ensures that each key has a specific role, restricting access based on security needs.

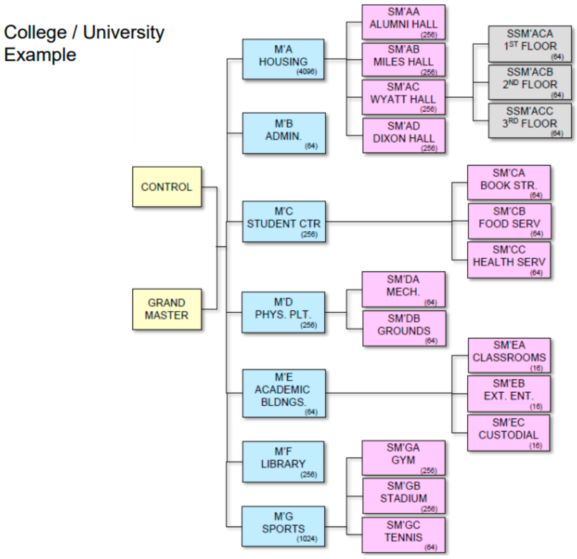


Figure 1: Exemple of Key System Hierarchies

2.3 Importance of Leaving No Trace

When compromising a security system like the BEST® IC core, it is critical to avoid leaving any trace of interference. Traditional intrusion methods—such as stealing keys, forcibly removing cores, or dismantling the system—can alert security personnel. If traces are left, the system manager can quickly respond by replacing the compromised cores, rendering any stolen keys or extracted information useless to the intruder. Therefore, a successful compromise of an IC core system requires subtlety and precision to avoid detection.

2.4 Understanding the Internal Mechanics of the IC Core System

The BEST® IC core system is engineered with mechanisms that resist unauthorized access, such as:

- **Special Key Features**: BEST® keys often include advanced security features, like the **PEAKS key**, which offers enhanced protection against unauthorized duplication and tampering.[1]

- **Cormax Patent Pins**: Another security element is the Cormax patent pin, designed to prevent key duplication and improve resistance to picking attempts.[2]

- **Dual Shearlines**: The IC core includes two separate shearlines—**the operator shearline** and **the control shearline**. A shearline is a specific alignment within the lock that allows rotation when the correct key is inserted. The dual shearlines make picking challenging, as it is unclear if a pin is set at the operator or the control shearline. This dual-shearline design makes the BEST® IC core system one of the most difficult locks for intruders to pick.

2.5 The Control Key's Role in Access

In a hierarchical system, the control key has a unique function, granting access to multiple cores within the system. In many cases, a control key can open even more locks than a master key, as it is used primarily by locksmiths and facility managers who need access to all cores. While some systems may feature multiple control keys, most configurations use a single control key for simplicity and security.

2.6 Extracting Information from a Core

Possession of a core alone can reveal critical information. With simple tools (which can be sourced online or created with a 3D printer), it is possible to open the core and examine the pin configuration inside. From the pin details, one can deduce:

- A list of potential keys that might operate the lock (often around 128 combinations), although most of these keys will not open other locks in the system.

- The exact control key for the core, providing access at the control level without the need for additional information.

[1] For more information, refer to `https://www.bestaccess.com/products/peaks-keys/`.

[2] For more details, see `https://www.bestaccess.com/products/cormax/`.

Moreover, the ability to close the core after examination is a critical advantage, allowing the core to be reinstalled without any visible signs of tampering. **This capability to identify the specific control key from a single core represents a significant security risk if left unaddressed.**

3 Methodology for Compromising the IC Core System

3.1 Obtaining an IC Core

The first step in this process is acquiring an IC core. Several factors often lead to IC cores being accessible due to staff negligence, lack of security training, or inappropriate use of padlocks. Some common scenarios include:

3.1.1 Example: Negligent Use of Padlocks

In some facilities, padlocks containing BEST® IC cores are used in low-security situations, such as locking trash containers. Maintenance personnel, who may need to access these containers frequently, often find it inconvenient to unlock and relock the padlock each time. As a result, they might leave the padlock unlocked, reasoning that it isn't necessary for something as trivial as a trash bin. This creates an opportunity to acquire the padlock without detection.

Furthermore, custodial staff may ignore the disappearance of such padlocks, assuming a colleague or locksmith has taken it legitimately. In some cases, they might even feel relieved not to have to manage the lock anymore. Even if they suspect the padlock was taken, they may avoid reporting it to prevent admitting their own negligence.

3.1.2 Example: Unsecured IC Cores During Construction or Renovation

During construction or renovation projects, it is common to install and later remove doors with IC cores. Often, door handles and other components containing IC cores are left unsupervised on-site overnight or over weekends. Occasionally, discarded door handles containing IC cores end up in trash bins.

Amid the chaos of construction, workers might assume the door handle was lost or misplaced. Here, the vulnerability lies in the inappropriate use of IC cores, which are crucial security components. Ideally, temporary IC cores with limited access would be used during construction, rather than cores tied to the main security hierarchy. This setup would reduce risk, especially since construction personnel are often contracted, making it difficult to ensure consistent security training.

3.1.3 Example: Lock Raking for Control Key Access

Obtaining an IC core without a key can sometimes be achieved through techniques like **lock raking** and other specialized picking methods. Lock raking involves inserting a rake tool and rapidly manipulating the pins inside the lock, creating a random, quick motion. This can sometimes align the pins at the shearline temporarily, allowing the lock to open without the control key. However, due to the dual-shearline design of IC cores, this technique can be challenging, as it's difficult to ensure that pins align specifically at the control shearline rather than the operator shearline.

To increase the chances of success, a variety of tools and approaches have been developed, particularly those targeting the control level of the IC core.

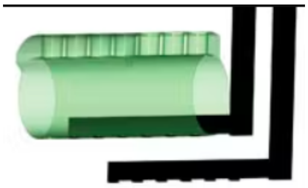


Figure 2: Tension bar [1]

One effective tool is a specially designed **tension bar** that interacts with the control shell of the IC core. Unlike traditional tension bars, which apply general pressure on the core, these bars are crafted to "bite" specifically into access holes located at the bottom of the control shell. This setup enables a more directed and controlled pressure on the control shearline, rather than on the operator shearline. Once inserted, the tension bar is maneuvered until it "drops" securely into these access holes, allowing pressure to be applied upward. By focusing force directly on the control shearline, this method significantly increases the chance of rotating the core at the control level, allowing for core removal.

Another technique involves using a **cut key**. A cut key is essentially a blank or minimally modified key with shallow cuts that allow it to be inserted and rotated freely within the IC core without engaging most pins. This blank movement provides flexibility, enabling slight manipulations of the pins with raking tools. The cut key method works because it allows the pins to rest near the correct alignment without specific depths. When combined with light pressure from a tension tool, the cut key lets the picker manipulate individual pins to align with the shearline, potentially bypassing the operator key and engaging the control level.

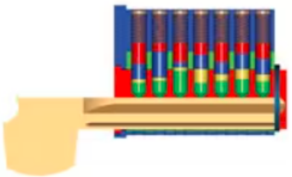


Figure 3: Cut key [1]

These techniques are best suited to low-traffic, isolated locations where they can be executed patiently and methodically. Targeting such locations allows for prolonged, focused work, essential given the time-consuming nature of these methods. For example, rarely used doors, like those leading to rooftops or mechanical rooms, are often ideal for such access attempts. Additionally, wearing high-visibility equipment, such as an orange vest, hard hat, and setting up caution tape, helps create an appearance of authorized maintenance, which can deter questioning from passersby, providing the necessary time and privacy for working with the IC core.

This combination of techniques and strategic planning leverages specific vulnerabilities in the IC core's design, maximizing the chance of a successful, trace-free core extraction.

3.2 Extracting the IC Core

Once a padlock or door handle containing an IC core is acquired (in the case you were not able to directly get an IC core), the next step is to remove the IC core itself. This can typically be achieved with simple tools, such as a hacksaw or other common equipment, allowing the IC core to be separated from its casing.

3.3 Extracting the Pins

With the IC core in hand, it's possible to extract the pins inside a IC core using 3D-printed tools. Methods for pin extraction can easily be found online. Once removed, the pins should be measured and recorded in a spreadsheet or other tracking system. This data will be essential for identifying the control key, a process detailed in Chapter 4.

3.4 Recreating the Control Key

To recreate the control key, you only need a caliper, a file, and a key-cutting tool like a Lishi cutter. Additionally, a 3D-printed guide can assist in shaping the key. Instructions for key duplication and fabrication are outlined in Chapter 5.

3.5 Using the Control Key to Access Additional Cores

With the control key in hand, the next step is to retrieve other IC cores from the facility. By using the control key to unlock and remove cores, pins can be extracted, analyzed, and documented. Proper reinstallation of pins and the IC core itself is crucial to avoid suspicion. Any mistakes in reassembly will result in a nonfunctional core, which might lead personnel to believe the core is defective rather than tampered with.

3.6 Identifying the Master Key

After gathering pin data from several IC cores (typically five or six), patterns begin to emerge that reveal which keys operate each core. This analysis identifies a set of potential keys (around 128), of which only one or two are likely to work across all the IC cores. The key common to each core is the master key, providing access to the entire system.

This methodology relies on subtlety and avoiding any detectable traces, as well as a careful understanding of the hierarchical structure of IC core security. Through systematic analysis and observation, one can identify the master key without compromising the system's physical integrity.

4 Determining the Control Key

The goal of this chapter is to extract the pins from the IC core and document them to identify the control key. This process involves specialized tools, precise measurements, and careful analysis of the pin system (A2, A3, A4). The following steps outline the procedure.

4.1 Tools for Pin Extraction

To extract the pins from the IC core, the following tools are recommended. While commercially available tools can be used, 3D-printed versions are more cost-effective and equally reliable.

- **Decapping Block**: This tool securely holds the core in place and simplifies the removal of the caps from the pin chambers. The commercial one costs $400, while the 3D-printed version costs $0.30.
- **Pin Unloader**: This tool is inserted into the core to push out the pins, springs, and caps during the extraction process. I use a screwdriver that is small enough as a pin unloader.
- **Pin Receiver**: This component collects the pins, springs, and caps after extraction, ensuring they remain organized and undamaged. The commercial one costs $400, while the 3D-printed version costs $0.40.

4.2 Extracting the Pins

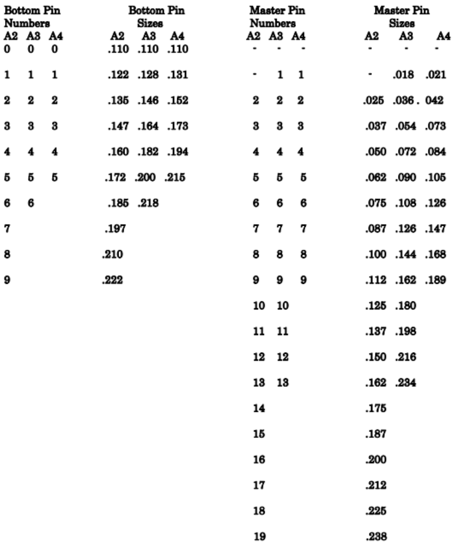
The pin extraction process involves the following steps:

1. Place the IC core into the **Decapping Block** to hold it firmly in place.
2. Insert the **Pin Unloader** into the cylinder of the core and align it with the first pin chamber.
3. Strike the Pin Unloader gently with a hammer to push the pin, spring, and cap out through the other side of the core.
4. The displaced components will fall into the **Pin Receiver**, where they can be collected for measurement and analysis.
5. Repeat this process for each of the seven chambers, taking care to handle the components delicately to avoid damage.

This systematic approach ensures all pins and their associated components are removed and organized for further evaluation.

4.3 Identifying the Pin System (A2, A3, A4)

To determine the pin system used in the IC core, you will need to measure the pins using a caliper and compare their lengths to the values in the provided table. The three systems—A2, A3, and A4—differ primarily in the number of pin depths:



Bottom Pin Numbers			Bottom Pin Sizes			Master Pin Numbers			Master Pin Sizes		
A2	A3	A4	A2	A3	A4	A2	A3	A4	A2	A3	A4
0	0	0	.110	.110	.110	-	-	-	-	-	-
1	1	1	.122	.128	.131	-	1	1	-	.018	.021
2	2	2	.135	.146	.152	2	2	2	.025	.036.	042
3	3	3	.147	.164	.173	3	3	3	.037	.054	.073
4	4	4	.160	.182	.194	4	4	4	.050	.072	.084
5	5	5	.172	.200	.215	5	5	5	.062	.090	.105
6	6		.185	.218		6	6	6	.075	.108	.126
7			.197			7	7	7	.087	.126	.147
8			.210			8	8	8	.100	.144	.168
9			.222			9	9	9	.112	.162	.189
						10	10		.125	.180	
						11	11		.137	.198	
						12	12		.150	.216	
						13	13		.162	.234	
						14			.175		
						15			.187		
						16			.200		
						17			.212		
						18			.225		
						19			.238		

Figure 4: Interchangeable Core Pin Size and Dimensions[2]

- **A2 System**: Total Stack Value of 23 and is the most common.
- **A3 System**: Total Stack Value of 16 pin, with slightly different measurements from A2.
- **A4 System**: Total Stack Value of 14 , making it the simplest of the three systems.

4.3.1 Measuring Pins

To identify the system:

1. Measure the length of several pins using a caliper with precision up to 0.001 inches.
2. Compare the measured values to the corresponding columns in the pin depth table. Note that there may be a small variation (±0.002 inches) between the actual pin length and the values in the table.
3. Select the value from the table that is closest to the measured length. If multiple pins match a particular system (e.g., A2, A3, or A4), it is likely that all pins in the IC core belong to the same system.

4.3.2 Pin Types and Configuration

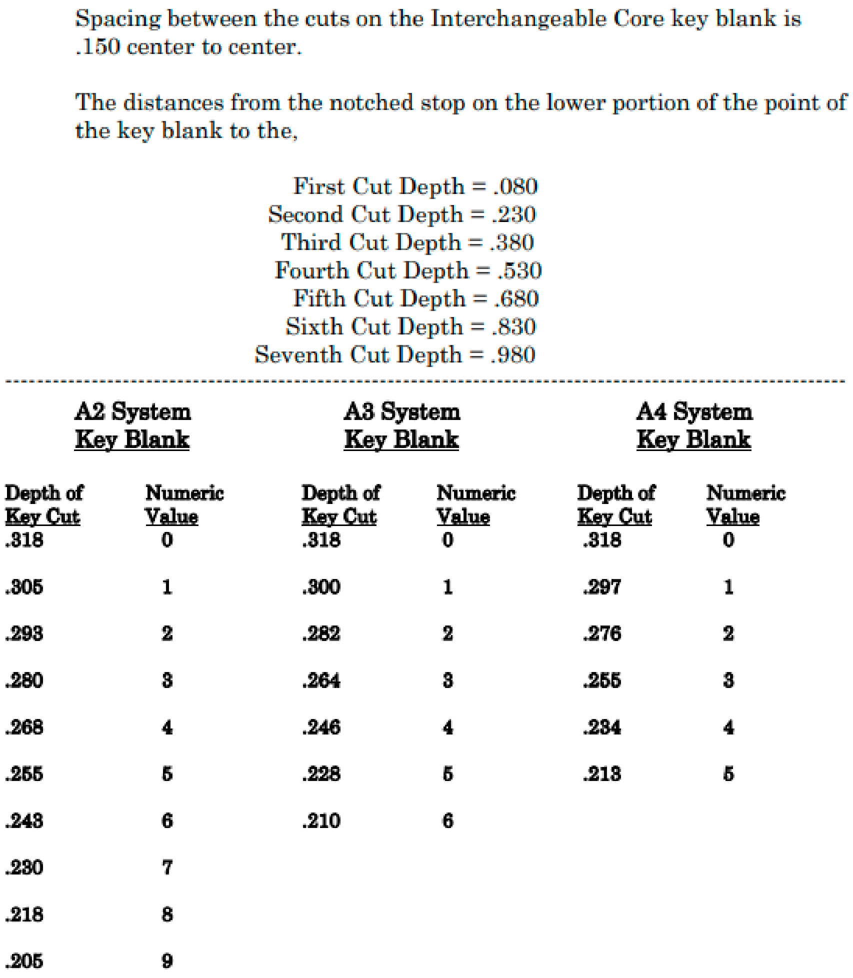
Each chamber of the IC core contains four pins:

- **Bottom Pin**: The bottom-most pin, which is pointed.
- **Some build-up Pins (Master pin)**: those are master pin and sometime control pin. Middle pins, cylindrical in shape, which act as spacers to allow different keys to operate the lock.
- **Top Pin** (Control pin): The top-most pin, cylindrical, used to engage the control shearline. Those are always control pin.

4.4 Documenting the Pins

After identifying the pin system, create a spreadsheet (e.g., in Excel or Google Sheets) to record the pin configuration. Use a grid format with 7 columns (for the 7 chambers) and 4 rows (for the 4 pins in each chamber):

Pin	1	2	3	4	5	6	7
Top							
B.-up 1							
B.-up 2							
Bottom							
Sum							



Spacing between the cuts on the Interchangeable Core key blank is .150 center to center.

The distances from the notched stop on the lower portion of the point of the key blank to the,

First Cut Depth = .080
Second Cut Depth = .230
Third Cut Depth = .380
Fourth Cut Depth = .530
Fifth Cut Depth = .680
Sixth Cut Depth = .830
Seventh Cut Depth = .980

A2 System Key Blank		A3 System Key Blank		A4 System Key Blank	
Depth of Key Cut	Numeric Value	Depth of Key Cut	Numeric Value	Depth of Key Cut	Numeric Value
.318	0	.318	0	.318	0
.305	1	.300	1	.297	1
.293	2	.282	2	.276	2
.280	3	.264	3	.255	3
.268	4	.246	4	.234	4
.255	5	.228	5	.213	5
.243	6	.210	6		
.230	7				
.218	8				
.205	9				

Figure 5: Interchangeable Core Key Blank Depth and Spacing Dimensions (Cut)[2]

Enter the measured values for each pin into the corresponding cell in the grid. This documentation will be crucial for calculating the control key in the next steps.

4.5 Filling the Table with Measured Pin Data

Once the pins are extracted and measured, the values are entered into the table row by row for each chamber. The steps to complete this process are as follows:

1. **Measure Each Pin:** Using a caliper, measure the length of each pin and record it in the corresponding cell of the table.

2. **Classify the Pin Type:**

   - If the pin is cylindrical and located in the middle of the stack, it is a **control pin** or a **master pin**. It's more often a master pin than a control pin.
   - If the pin is pointed and located at the bottom of the stack, it is a **bottom pin**.

3. **Determine the Pin Values:**

   - For **bottom pins**, compare the measured length to the *Interchangeable Core Pin Size and Dimensions* to determine its numeric value. Use the appropriate pin system (A2, A3, or A4)
   - For **control pin** or **master pins**, refer to the *Interchangeable Core Pin Size and Dimensions* to know if it's a master or a control pin (control pin are treated as bottom pin) (if it's on the top, it's a control pin) and find the numeric value that corresponds to the measured length. Use the appropriate pin system (A2, A3, or A4)

4. **Populate the Table:** Enter the numeric values into the appropriate cells for each pin type (top pin, build-up pin 1, build-up pin 2, and Bottom Pin). You may need to add some row in the case you have some master pin. it's possible that some chamber have only tree pin.Automation can speed up this process and reduce errors. Custom code can be written to automate the conversion of measured values into key cut depths, ensuring precision.

4.6 Calculating the Control Key Cut Values

The focus of this process is to determine the cuts needed for the **control key**. These values are derived exclusively from the numeric values of the **Control Pins**. The calculation involves the following:

1. Extract the numeric values of the Control Pins from the first table.

2. Convert these numeric values into the corresponding key cut depths using the *Key Cut Depth Chart.*

3. Record these depths sequentially to produce the cutting pattern for the control key.

4.7 Final Control Key Calculation

The control key cut pattern is represented as a sequence of numeric values that correspond to the depth of cuts required at each position. For example, if the Control Pin values for a 7-pin IC core are 3, 5, 2, 6, 4, 1, and 7, the resulting control key cut pattern will directly reflect these values in sequence.

$$\text{Control Key Cut Pattern: } 3 - 5 - 2 - 6 - 4 - 1 - 7$$

This calculated pattern can now be used to reproduce the control key, allowing the IC core to be unlocked at the control level.

4.8 Automation of the Process

For speed and accuracy, especially when dealing with multiple IC cores, automated scripts can be developed to handle:

- Pin length measurements.
- Classification of pins as bottom or master pins.
- Conversion of numeric values to key cut depths.
- Generation of control key cut patterns.

Such automation minimizes human error and ensures consistent results, enabling faster analysis and key reproduction.

5 Manual Key Duplication

Steps to Duplicate a Key

After completing Chapter 4 and determining the correct key cut sequence, the next step is to transform that sequence into a physical key.

5.1 Cutting the Key

Once you have your cutting guide, you can start making the key. There are a few ways to do this:

- **With a file:** You can file the key by hand. It takes time, because you need to file a little, then measure, then file again, and so on. You keep doing that until you reach the right depth.
- **With a Lishi cutter:** This tool is like a pair of pliers that you use to cut the key. It cuts quickly with small bevels, and saves time. But it's not perfect — you usually still need to use a file afterward to finish each cut properly. So you can cut fast with the Lishi, then tune with a file.

In the end, it doesn't matter how you cut — the most important thing is that each cut is at the right depth and well aligned.

5.2 Making a key

when manually duplicating a key, there are two critical dimensions to consider.

The first dimension is the *depth of each cut*—you need to ensure that each cut is made to the correct height. This can be achieved by using a caliper to measure how much material you are filing away. You file a bit, measure with the caliper, and repeat until you reach the exact depth needed.

The second dimension is the *position of each cut* along the length of the key blade. This positioning can be tricky to measure accurately with a caliper due to the shape of the key. To ensure that each cut is placed in the correct spot, it is helpful to use a guide.

You can create your own guide or repurpose an existing key that was professionally cut to serve as a template. This ensures that your cuts are aligned correctly along the blade. If you do not have access to a professionally cut key, you can also find or create a 3D-printed guide. Such a guide can help you with both the positioning and the depth of the cuts, making the process much easier and more precise.

5.3 Tape method for copying an existing key:

If you already have a working key and you want to copy it:

1. Take the original key and a blank,
2. Line them up perfectly,
3. Wrap them tightly with electrical tape frome the top (the head) to the tip of the blade,
4. un-tape the tape little by little as you make each cut,
5. This way you always see where to cut next, and the keys stay aligned.

It's simple, and some of the time, you don't even need to do final tuning — it just works.

5.4 Make slopes between cuts:

If one cut is very deep (like a 9) and the next one is shallow (like a 3), you need to make a small slope between the two. Otherwise, the key might get stuck when you try to insert it. That's why keys often look like little mountains — it helps the pins move up and down smoothly.

5.5 If you cut too deep:

Once you remove material from the key, you can't just put it back... except if you use solder. If the key is worth it (like a $20 key), you can:

1. Put solder where you went too deep,
2. Let it cool down,
3. Then file it again to the correct depth.

It's not super strong — the solder can break or get stuck in the lock — but it's good enough if you're careful.

5.6 If the key is bent:

Sometimes after using a Lishi cutter, the key isn't perfectly straight. You can hammer it gently on an anvil to fix it.

5.7 Clean sharp edges

Clean any sharp edges with steel wool or a file so the key goes in smoothly.

5.8 Testing the Key

When testing the key, insert it slowly, teeth by teeth, in an in-and-out motion to ensure that the key won't get stuck in the cylinder

6 Preventing Security Risks in IC Core Systems

6.1 Identifying the Core Problem

Many facilities rely on only two or three *control keys* for their entire interchangeable-core (IC) system. This creates a severe vulnerability: if a single lock goes missing—whether lost during maintenance, discarded, or stolen—security staff must assume the worst-case scenario, namely that someone could have extracted the control key and, from it, derived the master key.

In such a case, the entire key hierarchy would be compromised. Administrators would have to replace every lock and redistribute new keys to personnel. This process would be prohibitively time-consuming, extremely costly, and often impossible in practice. In reality, padlocks and cores go missing frequently, and many losses are never even reported. Thus, a single "missing" lock could, in theory, compromise an entire installation.

6.2 Why the Problem Is Critical

A padlock can easily change hands or end up forgotten in a storage cabinet. If that happens, and given what we now know from this report, the organization may be forced—at least on paper—to replace every master key and rekey every lock. Because each key and core is expensive, the total cost can reach millions of dollars. Faced with this absurd situation, practical measures are required to make IC-core systems meaningfully safer.

6.3 Some Recommended Preventive Measures

1. **Avoid using IC cores in padlocks.**
   Padlocks are portable and easy to lose. Staff frequently leave them unlocked out of convenience; a thief can also cut the shackle and remove the lock without leaving obvious evidence. In most cases the missing padlock would simply be replaced without raising suspicion. By contrast, a door handle cannot be removed without visible damage, which triggers an investigation. Therefore, IC cores should be used only where physical tampering would be evident.

2. **Use multiple control keys per facility.**
   Relying on a single control key for an entire building concentrates too much risk. Assign several control keys—for example, one per floor or per section—and design independent key hierarchies that do not share master or control keys. Modern computerized key-management systems make this feasible. Too often maintenance personnel are given multiple master keys that unintentionally overlap; that is proof of a lack of hierarchical diversification.

3. **Limit IC-core usage to essential areas.**
   Many IC cores are installed where they serve no real purpose, such as on tool chests or cabinets containing low-value items. The main advantage of an IC core is the

ability to rekey quickly; not every lock requires frequent rekeying. Excessive deployment increases interdependence: compromising one lock may force the replacement or rekeying of hundreds or even thousands of others, defeating the system's intended convenience. Ironically, overusing IC cores can destroy their benefit.

4. **Secure cores during construction or renovation.**
Construction sites are the worst source of exposures: handles, locks and cores circulate, are left unsupervised, or are discarded. Use temporary cores during construction, collect all cores at project end, and replace them with production cores before handing the site to staff. Create a dedicated control hierarchy for construction operations. Seriously: construction crews often handle cores worse than custodians — tighten that process.

5. **Other recommendations...**

6.4 Conclusion

BEST® IC-core systems exhibit a practical weakness that significantly reduces their effective security. Although marketed as high-security solutions, they—and likely similar products from other manufacturers—remain vulnerable to the loss or theft of a single core. It would be wise to investigate whether other vendors (e.g., Abloy and others selling IC cores) suffer from the same operational vulnerabilities.

Manufacturers advertise locks as "pick-proof" or highly secure, yet few invest seriously in research that tests and defeats their own mechanisms. **If real security depends on flawless organizational discipline—which often does not exist—then the protection is illusory.** Technical improvements help, but without strict usage rules and a well-designed key architecture, trivial physical attacks remain effective. Sometimes an attacker has an easier path by physically acquiring storage media than by attempting to bypass electronic protections when the physical key system is so fragile.

It is worth noting that BEST® products are used in government buildings, universities, and hospitals in the United States, according to their website.[3] The same concerns likely apply to critical infrastructure in Canada as well.

Final remark. Even if I discovered this myself, I do not claim to be the first to identify these techniques; in fact, others who work with IC cores are already aware and may have exploited these weaknesses. For example, Matt Blaze discussed this in 2003.[4] I do not think every locksmith working with IC cores realises this flaw or how easy it is to exploit. My aim is to make the problem explicit and show how easy it can be to compromise the BEST® IC core — with less than $150 (I have tested this personally). If practices do not change, organizations will keep replacing keys and locks while the real vulnerability persists. The problem is that it is much easier to compromise this system than it is to replace all the cylinders that have been compromised each time a lock goes missing. Worse, even if they change all the cylinders, an intruder need only take another cylinder later — which is not that hard.

[3] For more information, see `https://www.bestaccess.com/verticals/government/`.

[4] See Matt Blaze, *SFIC* (2003): `https://www.mattblaze.org/photos/misc/sfic/`. In his words: "A control key can then be decoded and cut that can remove other cores in the system. Decoding the control key is especially straightforward; it can be unambiguously determined from a single core simply by measuring the topmost pin of each pin stack. Hence the loss of a single lock in such systems is a very serious threat (padlocks are an especially vulnerable target)."

References

[1] Rod Oden, *Working with Interchangeable Cores When Keys are Not Available*, Locksmith Ledger, May 1, 2006. Available online at: `https://www.locksmithledger.com/locks/article/10230765/working-with-interchangeable-cores-when-keys-are-not-available`.

[2] Sargent Manufacturing Company, *Sargent 7300 Small Format Interchangeable Core Manual*, available at: `https://www.sopl.us/uploads/1/3/0/1/1301029/sargent_7300_small_format_interchangeable_core_manual.pdf`.

[3] Lock Surgeon, *Glossary of Terms*, available at: `https://www.locksurgeon.com/glossary.php`.

[4] Matt Blaze, *Notes on SFIC (Best) Interchangeable Core Locks*, 2003. Available online at: `https://www.mattblaze.org/photos/misc/sfic/`.