Door Key Theories on Lock Design

Lockpicker Perspectives on High Security

An original work by Ross Kinard (KnowTheBird)
Published and distributed by The Open Organisation of Lockpickers

Abstract:

This paper explores the theories and practical applications of lock design, focusing on how attackers exploit unintended information leaks and how security can be quantified probabilistically. It presents actionable mitigation strategies, including feedback obfuscation and staging, while assessing various access control systems for their strengths and weaknesses—particularly in resisting surreptitious and covert entry.

The discussion extends to real-world applications across commercial, governmental, and military security landscapes, evaluating industry standards and the product life cycle of high-security locks. Additionally, the paper provides an overview of physical attack methods and their countermeasures.

By examining theoretical limits, known attacks, and resilient defenses, this research bridges gaps between academic security analysis, locksport, and practical lock engineering, offering valuable insights for security professionals, engineers, manufacturers, policymakers, and the locksport community.

Revision Table:

Rev	Date	Revision Authors	Notes
-	Mar, 2025	Ross Kinard (KnowTheBird@gmail.com)	Initial Release

Acknowledgments and Thanks:

I would like to express my gratitude to Georgia Jim for their valuable insights on the Enclave. Special thanks to Phyxis and Alex Glandon for their thorough review and constructive feedback, which greatly enhanced this work. I also extend my appreciation to NØthing for their input on my designs and for introducing me to new high-security locks. Additionally, I would like to thank David Knauer for his review and support in getting this published. Their collective contributions have been instrumental in refining my research and deepening my understanding of advanced security mechanisms.

Ethical Disclosure:

This paper does not disclose any new security vulnerabilities or methods of attack beyond those already publicly known. All information regarding lock components and their usage was previously accessible through public sources. No financial compensation, gifts, or other forms of remuneration were received for the work presented. The content is presented solely for academic, professional, and ethical purposes, with the aim of advancing public knowledge in the fields of locks and physical security.

The authors and publishers do not endorse or encourage the misuse of security vulnerabilities or engagement in unlawful activities. Any practical application of the concepts discussed must comply with local laws and ethical standards.

The authors and publishers accept no liability for any losses, injuries, or damages resulting from the improper or unlawful use of the information provided.

Table of Contents

1. Introduction:

Access control systems are designed to restrict resources based on the presentation of valid credentials. These systems are prevalent in both physical and digital environments, where the credentials may range from physical keys to digital tokens, biometric data, or cryptographic keys. The fundamental function of an access control system is to ensure that the resource remains inaccessible until a valid key is presented, at which point access is granted.

In this paper, we focus on access control systems with the following characteristics:

1. The system does not provide access to a resource when an invalid key is presented.
2. The system does provide access to a resource when a valid key is presented.
3. The system independently validates the key, automating the authorization process without third-party intervention.

In this context, we define the system's operation as a function with two potential outcomes: access granted (authentication and authorization success), or access denied. Given this setup, an attacker can observe the outcome (whether access is granted) and use this information to determine whether they possess the correct key. This leads us to our first key theory: No access control system is unconditionally secure; they are probabilistically secure.

In cryptography, we can have systems which have information-theoretic security because we can make systems where the probability of one output being true is equal to the probability of any other output being true. We can also assemble such a system from access control system components. We could have three safes, each requiring a different key to open them, and each containing a different message, rock, paper, or scissors. In the absence of any other indicators of validity, any of the three messages could be true or false. However, in access control systems, restricting availability of the resource itself is also required. If we have two safes, one containing fool's gold and the other pure gold, the damage is not lessened when an attacker can access both.

To be useful, we want to create a bias and minimize the likelihood an attacker can access a resource without a valid key. It is that useful bias we intentionally design into an access control

system that also prevents it from being unconditionally secure. The probability of a key being valid is less than the probability of it being invalid. While it can be part of a larger information-theoretic secure system, the access control system itself will have probabilistic or conditional security, otherwise there would be no functional use.

Minimizing the likelihood an unauthorized user can provide a valid key depends on two main factors, the number keys in the system, and the secrecy of valid keys. To maximize probabilistic security, valid keys must be kept completely secret from an unauthorized user, and there must be significantly more possible keys to try than are valid. The *Probability of Access with a Random K*ey is:

$$P_r = \frac{Total\ Number\ of\ Valid\ Keys}{Total\ Number\ of\ Keys\ Possible}$$

This is the likelihood most often used to state a system's security; however, it is often misrepresentative because attackers don't usually rely on random guessing alone. Feedback from the system can significantly reduce the number of possible keys attackers need to test. The amount of reduction in the total number of keys depends on each access control system design and the attacker's ability to exploit it. This feedback is critical and will be discussed in greater detail in the following sections. For now, we will simply say P_f represents the *Probability of Access with Feedback*. Thus, the effective $Probability\ of\ Access$ for an attacker is:

$$P_a = max\left(P_r, P_f\right)$$

2. Systems And Feedback:

"*Before you make the key, study the lock.*" J.A. Konrath

Feedback is any observable response or emission from the access control system, such as whether a key is valid or invalid, or the time taken for the system to respond. Feedback can provide critical information to an attacker, helping them narrow down the valid key more quickly. However, the effectiveness of feedback depends on several factors, including the system design, the attacker's access to monitoring tools, and the interfaces available for probing. For the purpose of this paper, we classify top level attacks based on the attacker's access to system:

- Black Box: The attacker has no visibility into the internal workings of the system, and the only feedback they receive is whether the key is valid or invalid.
- Gray Box: The attacker has partial knowledge of the system's internal state or access to some components, allowing them to use more refined feedback.

- Clear Box: The attacker has full access to the internal state of the system, including all valid keys and key comparison outputs, which leads to a direct compromise of the system.

As attacks progress, the classification may change from black to gray to clear, depending on access the attacker gains. In this paper, these terms are in reference to the internal states and are not in reference to knowledge of system architecture. For high security systems, we follow Kerckhoffs's principle, which states "*a system should remain secure, even when everything about the system (except the keys) is public knowledge*", and Shannon's maxim, "*one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them*" [16].

Regarding these principles, we should also distinguish between producers of security systems and consumers. When we design a security system, we should do so anticipating the attacker knowing it as well as we do. Information will leak, and attackers will purchase or procure the system to reverse engineer it. Furthermore, transparency with third parties and getting reviews and certification will be critical to catching design and manufacturing flaws, such that consumers can trust the system.

Consumers of a security system are not in the same position. Publishing details about their security does not inherently improve their security posture, and in many cases, it could weaken it. It may well be wiser to keep the details for their security resources and usage internal to their organization. Third party security audits can provide private feedback and public certification.

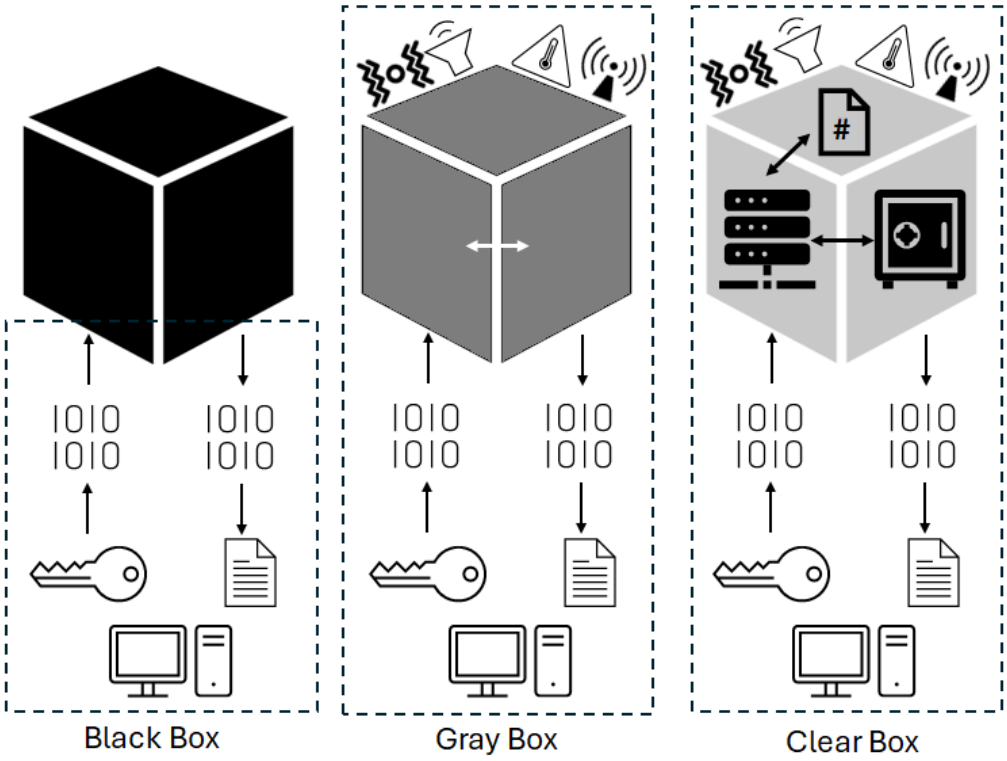

Figure 1. Feedback in Attackers Field of Observation

2.1 Black Boxes, Time Delays, and Logging:

In the black box system, the attacker's only feedback is the discrete output of a valid or invalid key. Due to the work-energy principle and second law of thermodynamics, the internal state change of a closed system always requires energy consumption and has resulting emissions, but if this feedback is outside an attacker's scope of observation, it is unusable.

The discrete output may need to be isolated, and time to response returned to the attacked may still need to be buffered to prevent feedback on the internal state of the system. This is covered in more detail later under Feedback Obfuscation below.

If there is no additional feedback outside of the discrete state of valid or invalid key, and no alternative bypass, the Probability of Access with Feedback will be equal to the Probability of Access with a Random Key and the fastest method of attack is equal to randomly selecting new keys to test.

A black box provides the ideal level of interface accessibility, and in many cases, it can be practically implemented if a portion of the system can be kept outside of the attacker's control or probing is made sufficiently difficult for modern tooling. Even though the system does not leak

information, it is not immune to attack. Temporary lock out features based on time of request or number of requests can greatly reduce the likelihood of a successful attack.

For example, we can set a time delay between attempts if we want to ensure an attacker has a 1% chance of success of brute forcing a key in 24 hours. The key is a 6-digit numeric pin (permutation with repetition), and the system takes 1ms to check pin validity.

$$T_a = Time,\ total\ time\ available\ for\ attack$$

$$T_e = Time,\ execution\ of\ testing\ each\ key$$

$$T_d = Time,\ delay\ between\ tests$$

$$K_a = Keys\ tested\ per\ attack$$

$$K_s = Keys,\ Total\ possible\ per\ keyspace$$

$$R_s = Ratio,\ likelihood\ of\ success\ per\ attack$$

Without any delay ($T_d = 0$) we can see the attacker could test every possible key 86 times:

$$T_a = \frac{1\ day}{attack} \times \frac{24\ hours}{1\ day} \times \frac{60\ min}{hour} \times \frac{60\ sec}{min} = \frac{86{,}400\ sec}{attack}$$

$$T_e = \frac{0.001\ sec}{key\ tested}$$

$$K_a = \frac{T_a}{T_e + T_d} = \frac{\left(\frac{86{,}400\ sec}{attack}\right)}{\left(\frac{0.001\ sec}{key\ tested}\right) + 0} = \frac{86.4E6\ keys\ tested}{attack}$$

$$K_s = \frac{10^6\ keys}{keyspace}$$

$$R_s = \frac{K_a}{K_s} = \left(\frac{86.4E6\ keys\ tested}{attack}\right) \div \left(\frac{10^6\ keys}{keyspace}\right) = \frac{86.4\ keyspaces\ tested}{attack}$$

We can use these same formulas to determine what time delay, T_d, to implement such that the likelihood of successful attack, R_s, is 1%.

$$T_d = \frac{T_a}{R_s K_s} - T_e = \frac{\left(\frac{86{,}400\ sec}{attack}\right)}{\left(\frac{0.010\ keyspaces\ tested}{attack}\right)\left(\frac{10^6\ keys}{keyspace}\right)} - \frac{0.001\ sec}{key\ tested} = \frac{8.640\ sec}{key\ tested}$$

$$R_s = \frac{\left(\frac{T_a}{T_e + T_d}\right)}{K_s} = \frac{\left(\frac{\left(\frac{86{,}400\ sec}{attack}\right)}{\left(\frac{0.001\ sec}{key\ tested}\right) + \left(\frac{8.640\ sec}{key\ tested}\right)}\right)}{\left(\frac{10^6\ keys}{keyspace}\right)} = \frac{0.010\ keyspaces\ tested}{attack}$$

$$R_s \times 100\% = 1\%\ likelihood\ of\ success\ per\ attack$$

Note, for many systems this will be an approximation, as the time to test a key depends on the key value. In later sections we will discuss how feedback and manipulation can reduce the total possible keys that need to be tested to determine the correct key. To determine the delay needed to slow manipulation by an attacker with feedback, you would leverage the equations above, adjusting the total number of keys to test, K_s to match your system. Use the total possible keyspace as we have done in this example when looking at "brute force" attacks, where the attacker will check every key in the keyspace.

To ensure an attacker does not bypass the time delay it should be required to have elapsed prior to key validation, or prior to accepting the next attempt's input, depending on the overall delay duration and the amount of latency authorized users are willing to accept. This can also be implemented such that an authorized user does not need to wait this period on each request, as seen below:

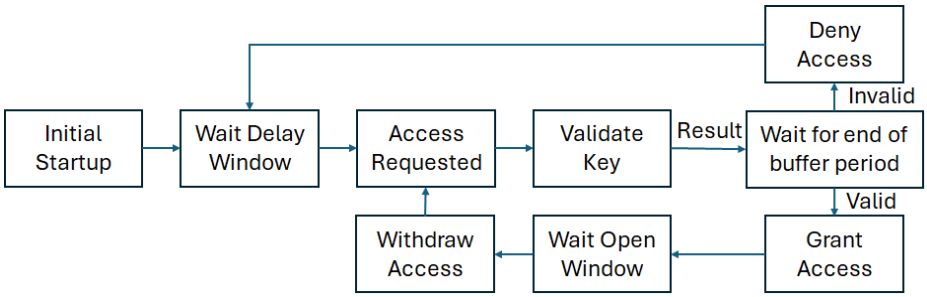

Figure 2. Time Delay Staging

Timelocks can also be used to set large periods of time where a lock cannot be opened. They were originally designed to prevent bank employees from opening (or being forced to open) a vault when the bank was closed, prior to banks using electronic alarm systems. Sargent & Greenleaf is credited with creating the first commercially successful design, the "Model 2", in 1874 [40], and variations are still used to this day for similar purposes, such as preventing employees from badging in on a shift they are not scheduled to work. This feature's utility is certainly case dependent, as some resources always need to be immediately available to an authorized user. For history and clock enthusiasts, Mark Frank's website provides an in-depth account of timelocks, with an extensive collection of high-resolution images and videos that highlight their components and movement [40].

Logging attempts is another valuable step we can take with a black box system to notify administrators and authorized users of the system that an attack is occurring or has taken place. Depending on priorities, this information may be used to further restrict the attacker's access to system interfaces (such as engaging longer delay window time periods), or to profile and identify the attacker. These logs can be electronically recorded and transferred via email or text message as part of a larger security information and event management (SIEM) system, or occur mechanically as is done for indicator, detector, counter, rotary, seal, and watchclock locking mechanisms. While not in common use, indicator and detector locks have been a part of high security locks for over 200 years, beginning with the Chubb Detector in 1818 [7]. Tamper detection seals can be seen in use as far back as 4400 BCE [8]. Logs and detectors can be quite simple and still be effective, but they also require additional management and inspection from authorized users.

Another important consideration for a black box system is the ability to reset keys. This can prevent a slow attack spread out over an extended period from being both undetected and successful. We will look at this closer when we look at human factors.

Restricting access to the system to prevent leaking information is a very valid approach and when done properly can be one of the most valuable layers of defense. It should not be easily dismissed. If an attacker can gain sufficient access to the system such that additional usable feedback is available, we classify it as a gray box. We will discuss it last as the most complex.

2.2 Clear Boxes and Damage Control:

In the clear box system, the attacker gains direct access to internal state data. In access control systems, internal state data will contain known valid keys, and key comparator outputs. When comparator outputs are available for the attackers to directly manipulate, the system can be bypassed. When this state data is available for an attacker to directly inspect, unencrypted keys may be decoded and compromised.

At this point detection (passive or active) triggering alarm systems, and/or relockers can become secondary methods of damage control. Detection is most reliable when always triggered by the final action granting access. An antique but high security mechanical example of this would be the Hobbs and Co. London Excise Paper Seal Padlock seen to the right. This was a padlock which shredded a paper seal as the bolt was retracted. Paper seals were issued by the government and restricted so they could not be easily replaced. Many variations of seal locks exist that show simple implementations that are effective.

Figure 3. Seal Padlock

Both mechanical and electronic relockers exist, whose purpose is to permanently restrict access to assets once it has been detected that the access control is compromised, or a destructive attack is occurring. This involves emplacing a detection system around the access control system, and a method for preventing access if a detection is triggered. For electronics one method is entering the valid keys for the access control system in a microcontrollers (MCU) SRAM, and then securing the MCU and its power source in an epoxy resin (potting), such that damage to the epoxy would likely result in power loss [11]. Additional sensors may be added to the epoxy which when triggered can in turn cut power. Epoxy resins are available specifically designed for x-ray resistance for additional protection. For mechanical systems this can include glass plates covering the access control components, that if shattered (ex, from drilling), engage a spring-loaded bolt (relocker) permanently securing the door. Bolts can be constructed using components with low melting points such that if a thermal torch is used to cut in, the mechanisms in place to retract the bolt are destroyed.

Zero Trust models are a cybersecurity framework designed to create secure systems under the assumption that attackers may already have insider access to the network. NIST SP 800-207 [14] offers comprehensive definitions and guidelines for implementing Zero Trust Architecture at the enterprise level. In general, the following Zero Trust principles can be applied to enhance damage control within our access control systems.

1) Never trust, always verify.
    - Always complete verification before granting access.
    - Require continuous verification from users to reauthenticate to retain access.
    - Hash all keys with salt and pepper to prevent easy reading or decoding with rainbow tables.
    - Encrypt all communication and resources and require the authenticated user to decrypt.
2) Only provide the least privilege needed for a task.

- Implement separate access control systems for distinct user groups, each tailored to the specific needs of the lowest-level user, role, or task.
- Restrict permissions within each access control system to ensure authorized users can access only what is necessary for their tasks.
- Set time-bound access permissions based on the expected use case and deadlines.

3) Monitor for and mitigate against attacks
   - Monitor and log both valid and invalid requests for resources.
   - Actively identify requests from users or devices which may be compromised.
   - Tailor responses or completely ignore a compromised source.

A common mechanical design violating the Zero Trust principle is the use of spring-loaded bolts and solenoid actuators such that a key is not required in all situations to retract a bolt. The designers assume because the bolt is not easily accessible, an attacker will not be able to interact with it, and trust that only the key cylinders cam will engage it. Because the key is not actually required, the attacker may be able to use magnets to pull the bolt back against the spring, use shim material to push it back, or use kinetic attacks (hitting or dropping the container) to get the bolt to bounce backward long enough to pull open the container door. On the other hand, systems where the bolt or shackle cannot be locked without the key (typically key retaining) are often implementing principles of zero trust and continuous verification, and are more resilient to bypass.

Another common example is with low security electronic safes. A reset button capable of changing the password for the safe is located inside the safe. It is assumed that the correct password must be entered and the door open in order to press the button. Attackers may use mounting holes, portholes for cabling, or backup master keyways to gain access to the switch, and toggle it while the door is still closed, allowing them to enter a new password for the safe. A zero trust model would request the user reenter their current password before setting a new one.

2.3 Gray Boxes and Limits on Keys vs. Feedback:

In the gray box system, the attacker has gained some additional feedback from the system reflecting its internal states. Due to the work-energy principle and second law of thermodynamics we know any system whose boundaries fall under the control of an attacker will provide feedback on the internal states of the system.

Before we look at the effect of this feedback, let's first understand the Total Number of Keys Possible when performing a brute force attack. This value and how we calculate it can change depending on the system. Below are some examples:

- Digi Lock Push Pad Lock – Simplex Combination
- Master Speed Dial Lock - Base 4 Hybrid, Permutation/Combination, Order Typically Matters
- Simplex L1000 Series – Permutation with simultaneous presses
- Android Password Pattern (grid lock) – Path with constraints, not a simple/pure permutation
- Typical Safe Combination, Sesame, Pin Tumbler, Dimple, Wafer, Lever, and Disc Detainers locks, Electronic PIN Codes, Cryptographic Keys - Permutation with Repetition

You can reference "The Five-Button Door Lock – Experiment and Discovery in Mathematics" or "Secure Your Phone with Pretty Pictures" for examples of calculating formulas for various systems, but a typical high security system will maximize the number of keys possible by using permutations where repetition is allowed. The equations used in this paper assume this is the case.

$$where\ n\ =\ total\ key\ length\ (mechanically\ equivalent\ to\ number\ of\ tumblers)$$

$$and\ where\ k\ =\ \ total\ number\ of\ unique\ symbols\ which\ may\ be\ used$$

$$(mechanically\ equivalent\ to\ number\ of\ positions\ per\ tumbler)$$

$$Total\ Number\ of\ Keys\ Possible\ =\ \ k^n$$

Note, with electronic passwords the total number of keys possible is often referred to using bits of entropy. [2] Bits of Entropy is the number of bits required to represent the total number of keys possible and is calculated as k^n. In a brute force attack, attempting to check every combination will take k^nattempts. There will be a greater than 50% chance of success after $\frac{k^n}{2}$ attempts have been made, which is equivalent to $2^{BitsOfEntropy-1}$.

The fundamental fault is most systems do not maintain k^n states to record the validity of each key. They share or compress validity information from multiple keys into a state, which means when that state is determined to be valid or not, we can tell if all keys associated with that state may be valid or not. This reduces the Total Number of Keys Possible needed to test.

Let's look at an example using a key with length of 3, and 3 unique symbols, and use a mechanical system with three tumblers (or electrically a base 3 storage system). The Total Number of Keys Possible = $3^3\ =\ 27$ and can be seen below:

111	112	113	121	122	123	131	132	133
211	212	213	221	222	223	231	232	233
311	312	313	321	322	323	331	332	333

Table 1. Possible Keys (Differs)

If we send an input and can monitor feedback indicating some state change, the longest series of steps in an attack for any given key is as follows:

1. 111 = locked means at least one value invalid
2. 112 = locked means at least one value invalid, no feedback means no state change
3. 113 = locked means at least one value invalid, no feedback means no state change
4. 123 = locked means at least one value invalid, no feedback means no state change
5. 133 = locked means at least one value invalid, no feedback means no state change
6. 233 = locked means at least one value invalid, no feedback means no state change, means position 1 must be 3
7. 333 = locked means at least one value invalid, feedback means position 1 value 3 is valid, means position 2 or 3 is invalid
8. 323 = locked means at least one value invalid, no feedback means no state change
9. 313 = locked means at least one value invalid, no feedback means no state change
10. 312 = locked means at least one value invalid, no feedback means no state change, position 3 must be 1
11. 311 = locked means at least one value invalid, feedback means position 3 value 1 is valid, means position 2 is invalid
12. 321 = locked means at least one value invalid, no feedback means no state change, position 2 must be 3
13. 331 = unlocked

These 13 attempts are significantly less than the 27 attempts required for a brute force attack. It is because there are only 8 states (2^3) representing 27 keys. This also assumes that the system only provides feedback from a single state preventing access at a given time. If we have a system where we can get feedback from any currently active state, we can further shorten the number of attempts. This would be equivalent to a mechanical pin tumbler, where sufficient torque is applied to cause multiple tumblers to bind simultaneously. Let's look at how many attempts this takes the longest possible case:

1. 111 = locked means at least one value invalid
2. 112 = locked means at least one value invalid, no feedback means no state change, means position 3 must be 3
3. 113 = locked means at least one value invalid, feedback means position 3 value 3 is valid, means position 2 or 3 is invalid
4. 123 = locked means at least one value invalid, feedback means state change, means position 2 must be 1 or 2
5. 223 = locked means at least one value invalid, no feedback means no state change, means position 1 must be 3

6. 323 = locked means at least one value invalid, feedback means position 1 value 3 is valid, means position 2 must be 1
7. 313 = unlocked

This assumes perfect interpretation of the feedback from the system. While that is generally very unlikely, it does provide us with the theoretical limit for the reduction in the total number of possible keys based on feedback. Those formulas are:

$$Total\ Number\ of\ Keys\ Possible\ with\ Feedback\ when\ Order\ Tested\ Matters$$

$$= \frac{n(n+1)(k-1)}{2} + 1$$

$$Total\ Number\ of\ Keys\ Possible\ with\ Feedback\ when\ Order\ Tested\ Does\ Not\ Matter$$

$$= n(k-1) + 1$$

This means to prevent useful feedback; we need a system where knowing the current internal states of the system is not of value. We can do this if the validity of one state does not provide information on the validity of any other state.

For a system to function as a true black box—one that does not leak any useful information about its internal states even when an attacker can observe all inputs and outputs—it must implement an injective function, such that the following conditions are held when evaluating keys:

1. The sum of unique internal states must be greater than or equal to the sum of possible unique keys.
2. No single internal state should contain information about multiple keys.

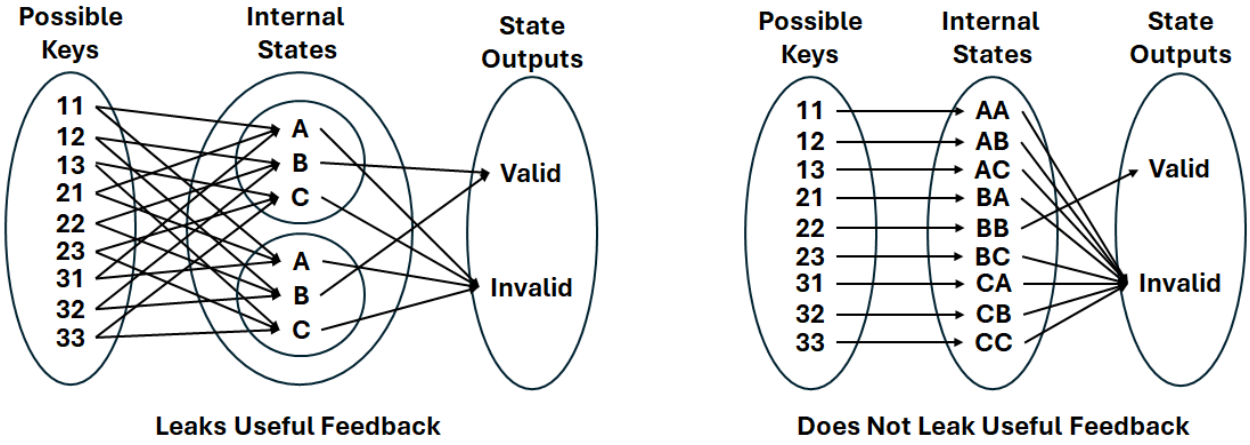

Figure 4. States Vs. Feedback

We could also express this as, let:

K be unique possible keys,

S be unique internal states the system can take.

O be the observable outputs.

$f(K) \mapsto S$ be the function mapping keys to internal states, it must be injective

$f(S) \twoheadrightarrow O$ be the function mapping states to outputs, will typically be non-injective surjective

for access control

To verify this more, let's evaluate the negative cases, Case 1 being, Suppose $S < K$

- If S represents the number of distinct internal configurations, but there are more possible keys than states, then at least two keys must share a common internal state.
- Let k_1 and k_2 be two distinct keys such that there is an internal state where:

$$f(k_1) = f(k_2)$$

- This means the system is collapsing or compressing different keys into the same internal state. A change in state results in observable energy leaving the system, so an attacker can see when state changes do or do not occur as the key changes. An attacker can observe the input-output behavior and detect patterns where multiple keys produce similar outputs.
- Thus, $S < K$ leads to key collisions that leak information.

For Case 2, let's suppose an internal state maps to more than one key

- Assume an internal state ss is associated with multiple different keys $k_1, k_2, ..., k_n$.

$$s \rightarrow \{k_1, k_2, ..., k_n\}$$

- This means that when an attacker observes the system at state S,changes the key K, he can apply the observed output to multiple keys, reducing the key search space. Instead of guessing among all K keys, the attacker now only needs to check a subset of possible keys.
- Thus, if one state maps to multiple keys, it leaks information.

Since both assumptions ($S < K$ or multiple-key state mappings) lead to contradictions, for a system to be a true black box, we can say it must satisfy our initial conditions.

Let's look at a few examples to see how this works, and the constraints with it.

In electronic systems, we can request a memory block, and for small passwords, this will not be unreasonable. If we have a 6-character numeric pin, we have $10^6 = 1$ million possible keys. If each key is represented by a bit, we can store this in 125 kilobytes of memory.

Now let's say we have an electronic access control system that takes a 14-character password which is case sensitive alphanumeric with special characters. The total number of keys possible is:

$$(26 + 26 + 10 + 33)^{14} = 4,876,749,791,155,298,590,087,890,625 \approx 4.88\ quintillion\ keys$$

If each bit uniquely represents one of the 4.88 quintillion keys, we will need 610,000 terabytes to store the true key value without leaking feedback.

The same space issues apply with mechanical systems. If we take a common keying system with 7 positions of 6 possible depths, we have $6^7 = 279{,}936$ possible keys. If each of these keys can be represented in an area of 0.25 mm^2, a total area of 1.12 m^2 will be required to represent those keys. While possible, this creates an exceptionally large space and material cost. Some readers familiar with Maximum Adjacent Cut Specification (MACS) may note this will play a significant role in the possible keys of pin tumbler locks. Please see the appendix for more detailed information on the specific effects of MACS.

Because the available space and memory will be constrained, we can also look at the effects of ensuring isolated key data states with a fixed memory budget. Let's say we have 128 bits available to store our valid key, what effects does each configuration have:

			Probability of Access with a Random Key:	*Probability of Access with Feedback where test order matters:*	*Probability of Access with Feedback where test order does not matter:*
Data States	K	N	P_r	$P_{f-ordered}$	$P_{f-unordered}$
Grey Box with Isolated Key	128	1	$\frac{1}{128}$	$\frac{1}{128}$	$\frac{1}{128}$
Grey Box with Shared Key	2	128	$\frac{1}{3.4\times10^{38}}$	$\frac{1}{8257}$	$\frac{1}{129}$

Table 2. States Vs. Probability of Access

What we learn is that even though we could create a system with no useful feedback for an attacker, for a fixed set of memory available, the system reduces the range of possible keys the attacker would need to try to below those required if we allowed the attackers useful feedback on the exponentially larger domain.

Considerations	Grey Box with Shared Key Data States	Grey Box with Isolated Key Data States
Susceptible to Side-Channel Attacks or Analysis (SPA, DPA, EMR, Timing, Manipulation)	Yes	No
Efficient use of Space and Material	Yes	No
For a fixed memory size, Higher Probability of Access (Higher likelihood of discovery)	No	Yes
Susceptible to Brute Force	Yes	Yes

Table 3. State Considerations

This means even though we can create systems with no useful feedback, for a fixed amount of memory, it can be more efficient and probabilistically secure to create ones sharing state data.

2.4 Feedback Obfuscation:

While fully isolating key data states may not be practical, selective feedback obfuscation can still enhance security. In the results above we see no, or restricted feedback can greatly increase the number of attempts required in a manipulation or analysis attack. For our assessment and design, we consider the worst cases where the attacker has sufficient skill, access, and

equipment to perfectly interpret all feedback. For our implementation, we take steps to lessen or obfuscate feedback.

Systems with limited feedback are often referred to as “quiet”. This is traditionally done by controlling manufacturing tolerances, adding false gates, staging and interlocks, and dampening.

2.4.1 Tolerances:

Generally speaking, by tightening the manufacturing tolerances in a mechanical system, the state changes will result in less movement, less energy transfer, and less feedback. This is not without risk though. Take a 5-pin tumbler lock with 6 cut-height positions. If the ordering of testing the pins matters, an attacker may need to test up to 76 key positions to open the lock (with perfect feedback interpretation). Because many of those 6 positions can be tested in a single motion of the pick, this means fewer than 76 motions will be required to open the lock for an attacker.

In the case of wide tolerances, we can expect only one pin to bind at a time, and applying additional torque will not result in multiple pins binding. If our 5-pin lock’s tolerance is so loose the pin height can be off by 1 position and still open, the attacker only needs to test 31 key positions.

On the other hand, if we tighten the tolerances enough, applying torque will cause multiple pins to bind and pins will simultaneously provide (damped) feedback when lifted. If the feedback is dampened enough such that the attacker often misses it, the total number of attempts required will increase.

However, if the feedback is not dampened enough to cause the attacker to miss it, the ability to bind multiple pins simultaneously means that manipulation ordering no longer matters, and the number of attempts can be reduced, in theory to a maximum of 26 attempts. If the tolerances become too tight, we will also begin to see the lock seize. This is to say, controlling tolerances can reduce feedback, but it will be an optimization problem with tradeoffs. Tightening allowable tolerances also results in additional tooling cost, in manufacturing the lock, and in cutting keys.

A rule of thumb for typical tolerance to allow components to move smoothly with some force is 0.1 mm, and a minimum of 0.061mm to prevent binding [30]. In the case of a plug inside a housing, this will be doubled for each side, so a minimum of 0.122 mm as the plug sits in the housing. In low security locks, the top of the plug may be flattened to match a flat pin at the sheer line, which can increase the gap at the sheer line an additional 0.127 mm to 0.381 mm [30]. Typical pin height differences will be 0.381mm to 0.584 mm. We can already see how a few of these configurations could lead to the extreme low tolerance case we discussed above. High security pin tumbler locks

will use a rounded plug to prevent this larger sheer line. The top of the key pins will be beveled to allow the plug to rotate, but the bevel will be minimized to improve pick resistance.

Part art, and part proof of concept, Digby Lock and Tool made a limited set of 100 custom “Bravo” locks showing how standard pin tumblers could be made difficult to pick by improving tolerances, even without difficult warding [43-44]. While it would not be called a high security lock, it was successful as a proof of concept showing tighter tolerances increased pick resistance [44-45].

Tolerance should also be considered for the access control housing itself. Gaps in the housing large enough to insert probes can allow systems to be decoded, or bypassed and can turn a black or gray box into a clear one. This certainly applies to both mechanical and electronic locking mechanisms. Requiring one or more 90 degree turns to pass through the interface of any two joints can significantly reduce the ability for an attacker to insert tooling. Access holes for mounting should also be considered a potential attack vector. When these holes are not all used for bolts during installation, it can provide predrilled access points. For example, in the past these mounting holes were used to insert tools able to toggle the password reset switch for electronic safes, allowing a new pin to be entered and the safe opened.

2.4.2 False Gates:

False Gates are “anti pick” features added to locks to provide misleading feedback to an attacker. They give the illusion that components are in the correct position when they are not. Typically called security pins in pin tumbler locks, we can sometimes see more elaborate hand crafted, and strategically placed security pins in the locksport’s challenge lock community than in the commercial market. Challenge Locks are specifically designed by lockpickers for the frustration and amusement of other lockpickers.

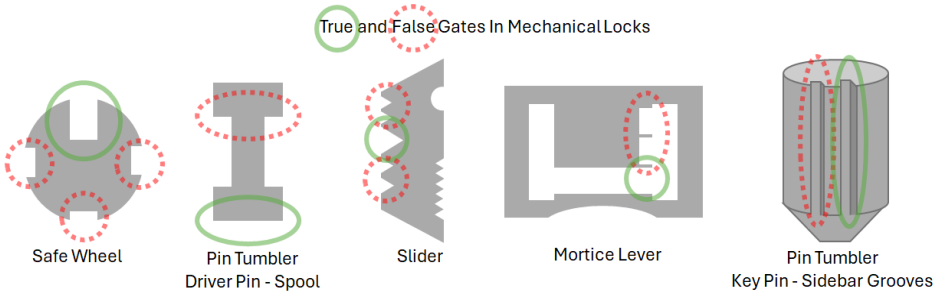

Figure 5. Common False Gates

In systems where order of testing does not matter, and the attacker can interpret all feedback, they do not increase the total number of attempts required. If every invalid position has a false gate, some cases may increase the number of times the attacker must switch the current tumbler (n)

being tested up to k(n-1). In systems where order of testing does not matter and the position k of n must be reset on each attempt, there is no increased workload on the attacker. In systems where ordering does matter, false gates can (but may not) increase the number of attempts required by the attacker. Each false gate's specific location in relation to true gates will affect how many more attempts may be required. They will be most effective when placed on the initial tumblers (n) which must be tested, and when they lead to additional false gates on the same tumbler under test. The absolute maximum the false gates can increase the number of attempts required occurs when:

1. Order of testing matters in the system
2. Every invalid position has a false gate.
3. Every false gate on a tumbler is cut such that it does not allow engagement of any false or true gates on any other tumbler next in the sequence of testing.
4. The false gate mimics true gates well enough the attacker cannot distinguish via feedback.
5. Only the true gate in a tumbler allows engagement with the next tumbler.

$$maximum\ additional\ attempts\ = \sum_{i=1}^{n}\left(\left(\sum_{j=3}^{k} k(n-i)\right)-1\right) = \frac{1}{2}n(k^2(n-1)-2k(n-1)-2)$$

This requires a level of quality control, and manufacturing precision the author is unaware of being used in any commercial product, but it shows careful usage of false gates can greatly increase attacker workload and give us guidance on designing with them. If we plot the number of possible keys with feedback where order of test matters without false gates (red) and with false gates (blue):

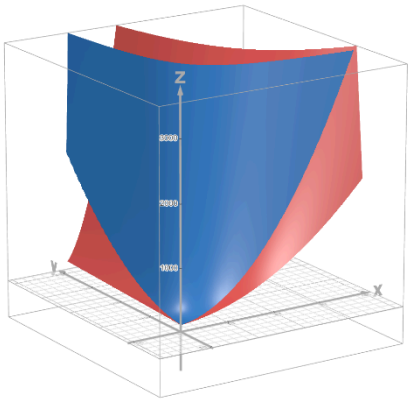

Figure 6. False Gate Effects

Here: x = n, y = k, and z = Number of Possible keys with feedback where test order matters.

$$\text{Red} = \frac{n(n+1)(k-1)}{2} + 1$$

$$\text{Blue} = \frac{n(n+1)(k-1)}{2} + 1 + \frac{1}{2}n(k^2(n-1)-2k(n-1)$$

What we see is that adding false gates increases the number of keys needed to test (as we expect), but we can also see that n still

plays a much greater role than k increasing possible keys with and without false gates.

Attackers can often determine if they are in a false gate both directly and indirectly with practice and experience. The following methods are commonly used:

- When counter rotation felt when applying pressure to a component
- Jiggle test applied, to identify which component is binding
- Unusually large “leaps” forward in the rotation of the lock (Pin Tumblers)
- Measuring cam gate width (Combination Safes)
- Total amount of lock rotation/movement

False gates can also function as indicators that progress is occurring manipulating the lock. In a pin tumbler, falling into a false set is a strong indication you have not overset a pin and are going in the correct direction, as in many locks only driver pins are milled to provide this effect, not key pins. This is leading to the practical benefits of false gates due to giving misleading feedback is often limited.

False gates typically (but not always) lock components in place such that counter rotation or reentering of the keying information is required to perform a test with a new key. In this way it is also a form of staging, which we look at more closely next. For now, suffice it to say, staging can play a greater role in the time it takes to evaluate a key than the number of additional keys which need to be tested due to false feedback. Without increasing the number of keys to test, they make the attack more difficult by increasing test time.

2.4.3 Staging and Interlocking components:

Each access control system has unique interfaces the attacker can monitor for feedback. Staging is a method which restricts the means in which feedback can be measured by decoupling the interface for key transfer from the components responsible for key validation prior to validation. In this process, feedback to multiple internal states via the interface is no longer directly measurable and massively reduced.

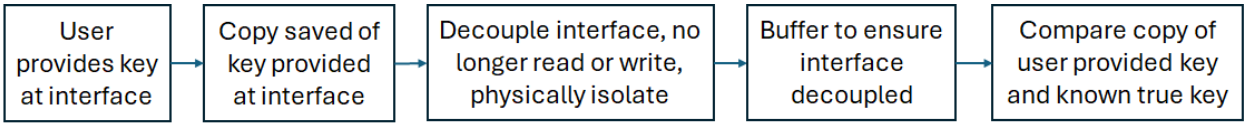

Figure 7. Staging Sequence

This is a common trivial process in electronic access control, but rare technology in mechanical systems. At the time of writing, this is an area ripe for future development. Andrew Magill's *Enclave* is a patent-pending design that incorporates staging in a pin tumbler lock [17], representing remarkable innovation in its field. A responsible designer, Magill sent prototypes to highly skilled lockpickers around the world. To date only one, Georgia Jim, has opened the Enclave fully populated. Below is his perspective on the feedback:

> "*Enclave uses 5 master wafers on top of each key pin to confuse feedback. The feedback of a set wafer is the same as a set pin. When pins are set to the incorrect height the core will turn in a deep false set that makes accessing the key pins impossible. When the pins are all set to the correct height a sidebar moves through the true gates on the driver pins allowing the core to turn and open the lock. As each driver pin is set to the correct height the sidebar moves forward incrementally and as a side effect the false set gets less deep which is counter intuitive to how most locks work. Once I understood that I used the depth of the false set combined with float picking to return the lock to as close to the neutral position as possible so that I could then lift another pin one wafer height and test the false set depth again.*
>
> *Ultimately, I used some creative cheating or OSINT to open the lock. Magill used the exact same key bitting for his CAD model of the lock as he did for the locks he sent out. This allowed me to set the correct number of wafers for each key pin. This is far easier said than done as you need as close to perfect tension control as you can muster to set the wafers the correct height and the correct binding order to prevent other wafers from dropping.*
>
> *This lock is realistically unpickable in my opinion as it would take hours of mapping and measuring the false set if the bitting isn't known. If a picture of the key could be copied, then something like a Lishi tool could be used very effectively to open the lock in much less time. The careful tension control would still be needed but the decoding grid would be extremely beneficial in opening the lock faster but would still need a skilled picker to do it."*
> Georgia Jim, 2025

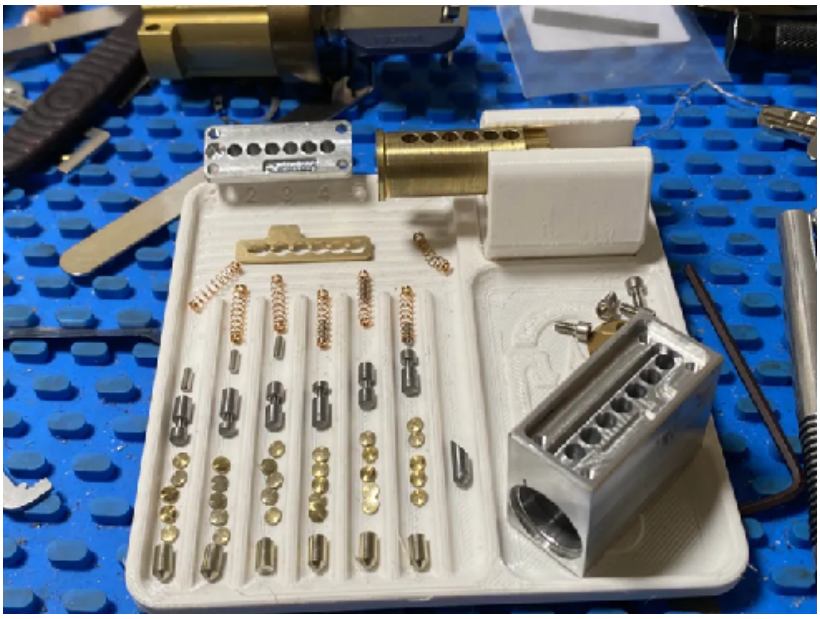

Figure 8. Internal Component of Enclave, Courtesy of Georgia Jim

Interlocking is related to staging in that it enforces sequence which must be followed. Interlocking may dampen feedback or introduce noise, but that is not its primary purpose. The primary purpose is to slow down the speed at which attackers can test keys. This sequence requires reset of key information before keys can continue to be tested. It does this by interlocking tumblers such that they cannot be individually moved prior to them being validated. The more key information that needs to be reset for each attempt, the more work will be required of the attacker to test a new key.

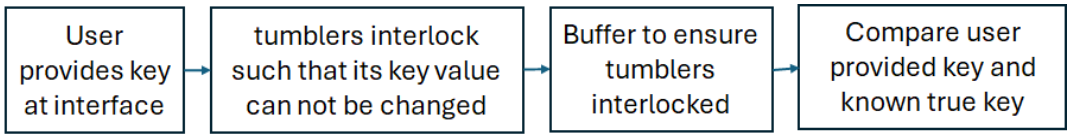

Figure 9. Interlocking Sequence

This often partially occurs indirectly as the result of adding false gates, and the degree of it highly correlates to the difficulty associated with them. For example, in a pin tumbler lock there are various security pins. A serrated pin and a gin pin (with counter milling in the plug) will both provide false feedback to an attacker. Due to how the large lip will interlock with the plug, the gin pin will require the plug to reset more than the serrated pin and will require more skill to reset without also resetting all the tumblers in the lock. The result is the gin pin is considered more difficult, and often associated with higher security locks.

Figure 10.
Security Pins,
Courtesy of MGSECURE

The Kwikset SmartKey (Gen II) interlocks all tumblers by using sliders with deep serrations in all false positions and a sidebar, but there is no buffer to ensure this occurs prior to validation, so light tension may be used to maneuver individual sliders. This can also occur as the indirect result of the locks method of setting tumblers, such as with combination dial safes. Perhaps one of the most well-known implementations of this process specifically for the security advantages is by the Abloy Protec Disc Blocking System (DBS) patented in 2001 [19].

The Abloy Protec is a disc detainer lock whose DBS interlocks all discs using return bars, prior to testing their positions with a sidebar. For more information, Han Fey provides an in-depth review of these locks in his “Evolution of Abloy” series. While attacks have been reported successful by exploiting regions where the DBS does not fully engage [36], these are non-trivial requiring advanced skill and custom tooling. The Fichet Bauche 787 also contains a method for interlocking its discs, as seen below. Note how components 25 and 26 interact with 8:

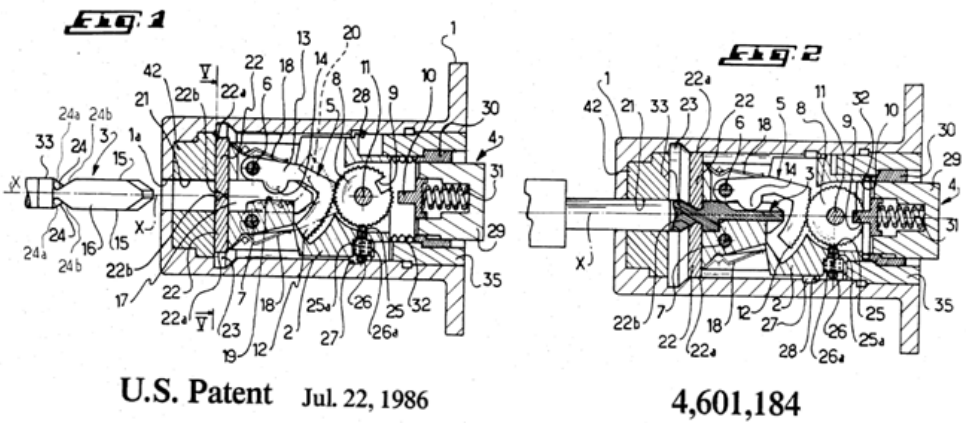

Figure 11. Fichet Bauche 787 Patent Drawings

The Zoned Adherence Keyway (ZAK) is a public open hardware design under a CC BY 4.0 license demonstrating both staging and interlocking with a geared form of disc detainer [18]. A driver and zoning disc enforce stages which must be followed. These stages prevent interaction between the Locking Bar and Gate Gear until all Gate Discs are first interlocked and the Gate Gear is decoupled from the Key Gear via an Axle Gear. This design is not in production, but a demonstrator of how these systems can be integrated for redundancy in a zero-trust system and will hopefully inspire future innovation.

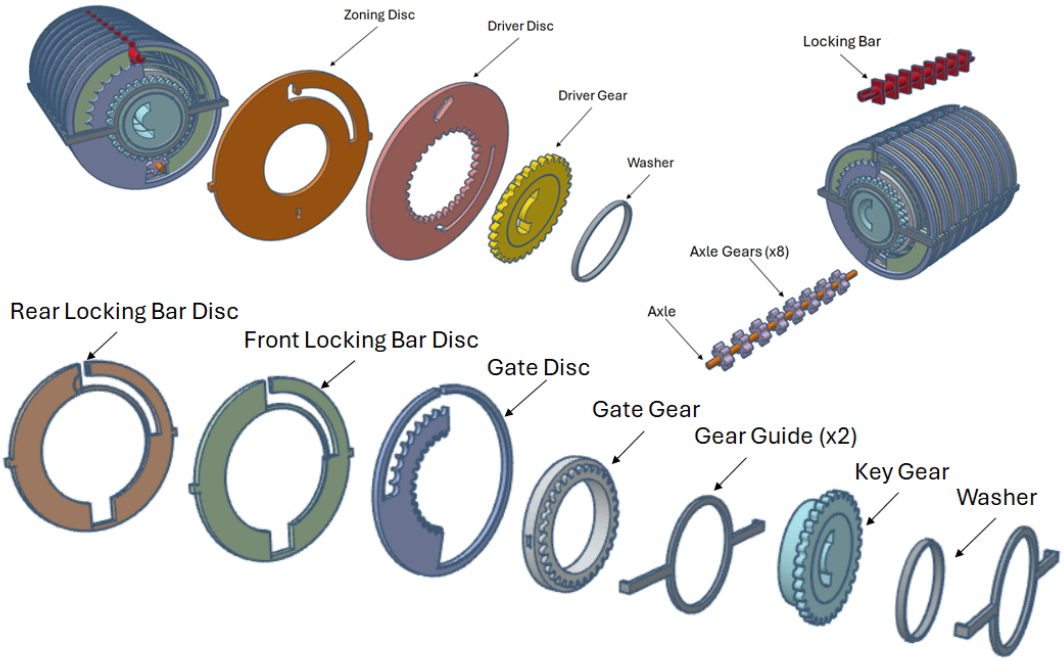

Figure 12. Zoned Adherence Keyway (ZAK) Components

2.4.4 Dampening and Buffering:

In mechanical locks, dampening output is rare but not nonexistent. Group 1 safe locks like the LAGARD 1985 may use springs to dampen the force of the fence on the dial pack. The DOM Diamant is a disc detainer which uses rubber spacers between discs to dampen feedback through disc rotation [20]. The Ingersoll 10 lever + sidebar lock uses a rubber gasket on the plug to dampen feedback through cylinder rotation [20]. Some new lockpickers report more difficulty with locks with sprung cores, which apply counter rotational force to the plug, but this will not typically have a significant effect for an experienced attacker. Typically, attackers for mechanical systems can apply more force on the locking bar when they need to increase feedback. They can do this until they begin to seize components or damage the lock (if they are concerned with surreptitious entry).

Reverse sidebars are a mechanical design that allows a lock to isolate torque applied on a cylinder lock from the force applied to the tumblers (typically sliders or wafers). These work by using a sidebar which has its own internal springs to push it to engage with the tumblers when they are at the correct position. Properly implemented the springs are light enough that 1) the springs for the individual tumblers are strong enough to overcome the sidebar springs, and 2) there is little to no feedback an attacker can use to decode. The portion of the sidebar that engages with the core is square shaped, such that any torque applied to the plug when the tumblers are at the incorrect position is orthogonal to the direction of movement for the sidebar, the sidebar binds in place, and little to no force is transferred to the tumblers. [33]

The reverse sidebar does not remove all feedback, but typically require more advanced picking techniques to open, which either 1) involve finding a method to apply an external force to the sidebar, or 2) using the small amount of feedback from the reverse sidebar setting the wafers to the correct position, and developing tools to hold the wafers in place until they are all at the correct position. As more are set to the correct position, feedback may improve. [34] A successful implementation of reverse sidebars is in the Yuema 750, which also has a unique feature where its core can freely spin over 360 degrees continuously when the incorrect key is used [35].

In electronic systems, timing analysis attacks may be performed monitoring response and delay times. Software can implement process schedulers to ensure responses are only sent at fixed intervals. The interval should contain a buffer of time set aside to allow any different comparator paths to complete.

Simple Power Analysis (SPA) attacks are performed by monitoring power consumption of a device to get feedback on internal states. "*String or memory comparison operations typically perform a conditional branch when a mismatch is found. This conditional branching causes large SPA (and sometimes timing) characteristics*." [25]. This is an issue, as it is exactly the type of operation we perform in access control systems. We can prevent it completely using Isolated Key Data States by implementing lookup tables, where keys point to the index of memory containing the validation as seen below:

```
#include <stdio.h>
// Macros from https://stackoverflow.com/questions/2525310
#define SetBit(A,k)     ( A[(k)/32] |= (1 << ((k)%32)) )
#define IsBitSet(A,k)    ( A[(k)/32] & (1 << ((k)%32)) )

int main() {
   // int is 4 bytes or 32 bits, so for this example only one
   // needed in the array, but typically we would use more
```

```
    int UniqueData[1] = {0};
    SetBit(UniqueData,7);

    int UserProvideValue;
    printf("Enter Your Password / Key: \n");
    scanf("%d", &UserProvideValue);

    if IsBitSet(UniqueData,UserProvideValue) {
        printf("Open Lock \n");
    } else {
        printf("Do Not Open Lock \n");
    }
    return 0;
}
```

The problem as discussed under gray boxes is this greatly restricts the number of keys we can use for a given amount of memory.

Instead, we can avoid conditional algorithms which may exit early depending on comparison operations and use iterative algorithms that will take similar amounts of time and energy regardless of differences in the keys.

```
bool isEqual(uint8_t const * const InputKeyHash,
             uint8_t const * const SecretKeyHash,
             const uint8_t HashLength) {
    uint8_t result = 0;
    for (uint8_t i = 0; i < HashLength; i++) {
      result |= InputKeyHash[i] ^ SecretKeyHash[i];
    }
    return result == 0;
}
```

A similar algorithm can be used in cases where hashes are not used (not recommended) and keys of potentially different length are compared. Make the user key and secret key buffers of equal length to the maximum key size. When storing the secret key, pad any remaining bytes in the secret key buffer with 1s (do not repeat this operation during comparison). When a user key is received, pad any remaining bytes in the user key buffer with 0. Then the above iterative XOR can be used.

To help mitigate this at a hardware level we can use electromagnetic shielding material around the access control system container to create a faraday cage, and improve filters used on the power supplies [26]. Optocouplers can be used to decouple internal power and electromagnetic information from data transfer lines. Amphenol has product lines of connectors with built in filters

that can be used for data and power interfaces to reduce EMI for various applications, including TEMPEST equipment [27]. Companies such as RAMBUS also offer dedicated integrated circuitry and accompanying software libraries for cryptographic algorithms that are resistant to SPA and DPA [28]. These circuits attempt to limit leakage by refactoring firmware and hardware and inducing random noise.

2.4.5 Noise Injection:

False gates are generally the source of noise in mechanical systems. The Chubb Mark IV Manifoil is a combination safe which forces two spring loaded rollers on the primary cam and a plastic tube around the spindle specifically for the purpose of adding noise [35]. There has been some work started to create a lockpicking game which introduces vibrations and random plug rotations, but this is not intended to be for high security locks.

Electronic systems can introduce random noise to assist resistance to SPA and DPA attacks. Dedicated circuity is available from companies such as RAMBUS [28] for this purpose. MCUs or FPGAs could be attached to circuity to generate random noise irrespective of the access control system logic, but the effectiveness will be highly dependent on both randomness and ability to mask as a possibly valid signal. Hardware clock rates can also be designed to fluctuate. It is not a trivial problem though and designers should be extremely cautious to not rely on noise injection alone for protection, as many statistical attack methods exist for these problems [25].

3. Keys and Interdependence

While most access control systems have one locking mechanism and one key, many organizations will require different ways to manage risk and access with multiple users. In a high voltage power plant, it may be required that no one can disengage locks to energize the system if any user has unlocked an electrical maintenance panel. Banks commonly employ dual custody locks on safety deposit boxes to reduce the risk of fraud. Hotels need to allow maids and maintenance in and to be able to replace lost keys quickly and easily.

Keys	Locking Mechanisms which can grant access	Usage Notes
Single	Single	Typical Use Case
Single	Multiple – Interdependent	Common in Higher Security Systems
Single	Multiple – Independent	Universal Keys, Storeroom, Classroom, and Institutional Locks, Trapped Keying
Multiple	Single	Master Keying, Maison Keying
Multiple*	Multiple – Interdependent	Two Person Integrity (TPI), Dual Custody

Multiple	Multiple – Independent	Master Keying, Maid Key, Change Keys

- For TPI “split key” cases, the key portions can be thought of as distinct keys.

Table 4.Common Access Control Key Configurations

3.1 Single Key - Patents and Restrictions

A single key and a single locking mechanism is the simplest and most common case and is what this paper has focused on so far. There is no need to describe that more. Instead, we will take a moment to discuss key secrecy, and how single keys remain single keys.

Many years ago, when I was still in preschool, my mother needed something from the store, but she was not able to leave the apartment at the time. The next-door neighbor offered to go to the store for her and get it but would need to borrow her car. It seemed the neighbor was being helpful and friendly, so she gave him her keys. She did not realize in the short period between him leaving and returning with the items, that he had gotten a copy of her apartment key made. Many months later he would fail at an attempted kidnapping. The resulting search of his apartment would reveal he had used the key to enter her apartment, steal family photos, and had set up string through the air vents to pull over cans in the pantry in the middle of the night and watch her investigate. Today my mother never hands out a key unless she needs to (ex: annual car inspections), and then she only hands out a single key.

Part of the reason making a copy of the key was so easy, was the apartments used Kwikset locks. These are common residential locks where a key can be made by any locksmith and at most local hardware stores. Some companies such as Bowley prevent this by offering unique key shapes for extremely restricted keyways, only selling cut keys to registered owners, and only selling key cuts matching locks they have previously purchased [73].

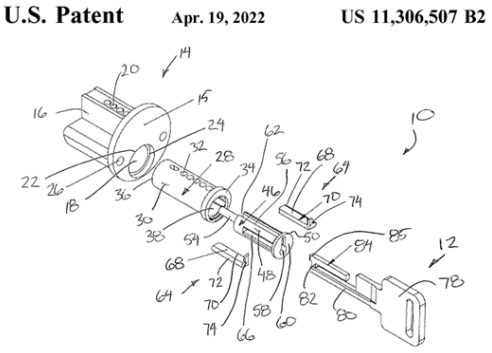

Figure 13. Original Bowley Patent with Novel Sidebar

Another common method to further prevent unauthorized duplication is key control via patents. “Do Not Duplicate” stamped on a key is a request, and on its own, not legally binding. Patents are legally enforceable though. By designing patentable keys, manufacturers can limit the legal

manufacturing of keys to their own factories (restricted keys) or approved dealers (semi restricted keys). Medeco offers a variety of restricted and semi restricted keys for the public, depending on the customers' needs; these can include requiring both an authorization card and matching ID [55]. Medeco also has lines of restricted keys for the U.S. military, where only cut keys are shipped directly from the manufacturer to the military base.

Of course, there are many illegal methods by which patented keys can still be copied, but by making these methods illegal, more burden is put on an attacker's skills and resources. Photos of keys can be used to cut a key by hand. This technique has also been shown to compromise systems where keys were restricted, but vendors posted photos of the true keys online. This was the case with Diebold voting machines in 2007, where the photo of a key to a low security wafer lock with loose tolerances was posted publicly. Molding and casting provide a low-cost method capable of duplicating many keys quickly. For attackers with more financial resources and access to the key, there are key duplicating machines such as the Easy Entrie Key Blank Milling Machine by KEYMAX capable of duplicating warding from patented keys on metal bar stock [54]. More recently 3D printing keys has become popular, with STL files publicly available for various key profiles and master key systems.

Some keys further restrict unauthorized duplicates by embedding electronic chips which need to be programmed, or interactive elements. Interactive key elements that are required to engage with the lock to set tumblers, such as the Mul-T-Lock Interactive, will be more resistant to key duplication than those which use passive pins, like the FAB 1000, or primarily decorative interactive components, like in the An Tun.

Electronic devices generating Time-Based One-Time passwords (TOTP) tokens, such as RSA SecureID, can provide high levels of resistance to copying. If the token is copied, it quickly expires. If the hardware is taken, there are anti-tamper features which can erase the seed should damage occur [11]. This has another advantage in that there is no significant change to the level of security even after any patents have expired.

Figure 14. RSA SecureID TOTP

3.2 Single Key - Multiple Interdependent Locking Mechanisms

When we say a single key with multiple interdependent locking mechanisms, we mean multiple methods of authenticating the same key. This can be thought of as hybrid blends of security

features, such as a lock with pin tumbler locks, that also most rotate pins to engage a sidebar (Medeco), or orient magnetic discs (EVVA MCS), or engage sliders with a sidebar (RUKO Garant+).

The advantage of this is not the number of possible keys, that can be done with a single type of locking mechanism. The advantage of this is layered security. If a critical vulnerability is found for one locking mechanism, the system can still rely on the secondary mechanism to provide some security. While bumping Medeco locks is possible, it is made more difficult than a standard pin tumbler by its rotating pins [58]. To bump open the RUKO Garant+, the sliders would also need to be properly set.

The MCS cannot be bumped as the pins are passive to restrict unauthorized keys, and the primary security is through the magnetic discs. The magnetic discs do provide strong resistance to manipulation, however, because the passive pins offer little security, they cannot provide any real crutch if the magnetic discs are compromised. This is to also note, multiple locking mechanisms will not always offer a significant advantage over a single mechanism. The security MCS would likely not be significantly impacted if the passive pins were removed.

Having multiple locking mechanisms also required attackers to develop additional skills. They may be very proficient at single pin picking pin tumblers, but poor at picking sliders. Finding new ways to integrate existing and proven security mechanisms may be easier and more reliable than trying to create a novel one. If it's decided to use multiple mechanisms, we should try to use multiple high security mechanisms, rather than trying to make high security locks by interconnecting mechanisms which have been proven to be weak. This may also assist in getting patents for key control.

3.3 Single Key - Multiple Independent Locking Mechanisms

A universal key with multiple independent locking mechanisms refers to multiple locks keyed alike (KA) to open from a single key. This is very common in residential settings where you have multiple doors to the home which use the same key. In commercial settings, janitor, maintenance and supply closets often share a single key. Hospitality may use a single master key as a backup for all in room hotel safes. Industrial settings may use padlocks keyed alike for storage units or shipping containers. Fleet management and heavy equipment will often have vehicles keyed alike. Emergency fire, rescue, and first responders may have keys to emergency key boxes for nondestructive access to buildings. The appeal is its low cost and simplicity to implement and manage.

The downstream consequence is that the security is significantly weakened. If an attacker gains a key, they have access to more resources. If an attacker can get access to any of the locks (purchasing new, used, trash, or stealing), the lock can be reverse engineered to determine the key

for all the remaining locks. If the attacker can get access to multiple locks keyed the same, they may be able to increase the speed at which they test keys. If this kind of system is desired, the security can be improved by having the access system also trigger some form of logging, recording, or alarm.
DeviantOllam points out some less common but important door and latch cases to be aware of in [60]. In it he discusses cases where it may be desired to have a single door, with the same locking mechanism on both sides. These are summarized in the table below.

Latch Type	Exterior Handle	Interior Handle	Use Case	Limitations
Storeroom Lock	Always Requires Key	Always Requires Key	Resistant to under and over tool bypass	Per fire and building codes, may be Illegal
Classroom Lock	May Require Key	Never Requires Key	Allow teacher to lock exterior from interior	In emergency, needs a key, and can bypass
Institutional Lock	May Require Key	Always Requires Key	Corrections, Nursing Homes, Hospitals	Fire and safety risks to interior occupants

Table 5. Specials Cases of Latches

Lastly, trapped key interlocking systems are designed for industrial and high-security environments where enforcing a sequence of operations is essential [59]. These systems use a single key that can only be removed and used in another lock after specific conditions are met, such as powering down equipment, stopping movement, or closing a valve. This ensures users follow predefined safety or security procedures. Since trapped key interlocking systems typically do not require electricity or centralized management software, they are more reliable in harsh or remote environments.

Depending on the design, the locking mechanisms in a trapped key system can be independent or partially interdependent (hybrid). A hybrid system links the state of one lock to the next, such as requiring a valve to be closed before the key can be turned in another lock. Independent systems, on the other hand, allow each lock to function autonomously, even if the key remains active in multiple parts of the system. Hybrid systems offer additional security against unauthorized attempts to bypass the system or unsafe operational states. To further enhance security, using restricted keys can prevent unauthorized duplication and ensure adherence to key control policies. On rare occasions the hybrid system appears to be used to increase the number of cylinders which need to be picked, as is the case with the "LIKA" dual cylinder, double sided dimple lock [72].

3.4 Multiple Keys – Single Locking Mechanism

In commercial, educational, and institutional settings, you will often see cases where multiple unique keys with distinct bitting can open a single lock. Depending on the key, it may also open

other doors in the building. These systems typically use Master Keying or Maison Keying. Of course, anytime we let multiple keys open a system the probability of access for an attacker will increase.

For Master keying, we will first look at some general principles to better understand some limitations and risks. There are various methods that could be used to implement the equivalent logic of comparing multiple keys. For example, per the distributive property of Boolean algebra:

$$where\ k_1 = ABCD,\ and\ k_2 = AB\overline{CD}$$

$$ABCD + AB\overline{CD} = AB(CD + \overline{CD})$$

$$Possible\ Keys = k^n,\ so\ for\ a\ boolean\ key\ with\ 4\ inputs = 2^4$$

$$Probability\ of\ Access\ (no\ feedback) =$$

$$P_r(ABCD + AB\overline{CD}) = \frac{1}{2^4} + \frac{1}{2^4} = \frac{1}{2^2}\left(\left(\frac{1}{2^2}\right) + \left(\frac{1}{2^2}\right)\right)$$

Below we can see a few different hardware circuit implementations of the same logic.

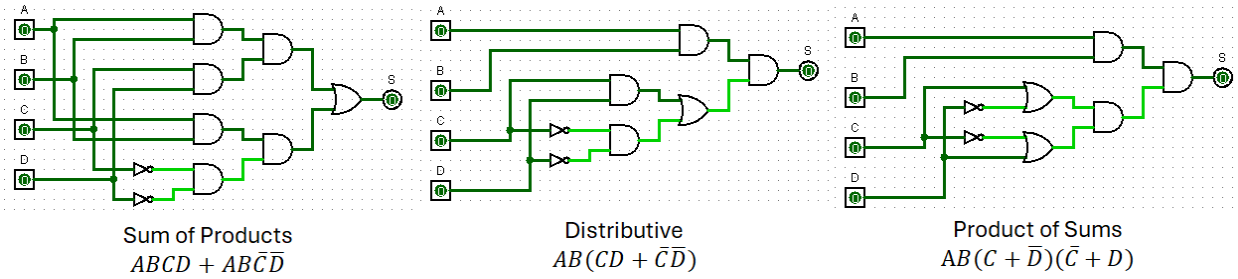

Figure 15. Circuits Leaking Feedback

From the standpoint of randomly testing keys without any feedback, each of these circuits would provide the same probability of access according to the equations above. If an attacker had access to the power supplies and could monitor power consumption, all of these would be susceptible to power analysis attacks (in these cases power consumption dropping means further from a valid key). Additional information could be gained about the master keying from the propagation delays. Buffers could be added for the propagation delays, and the gates could be chosen to minimize feedback, but there will still be some feedback. What this is leading to, is that to completely prevent information leakage about the master keying system we need to follow the same rules as

we do to prevent leaking information on a single key (previously discussed in section 2.3, gray boxes).

When there are the same number of unique states as there are possible keys, we can create master key systems that do not leak information. Even though multiple keys are now valid, we do not need to increase the number of states to represent them. For example, both the following circuits would prevent feedback.

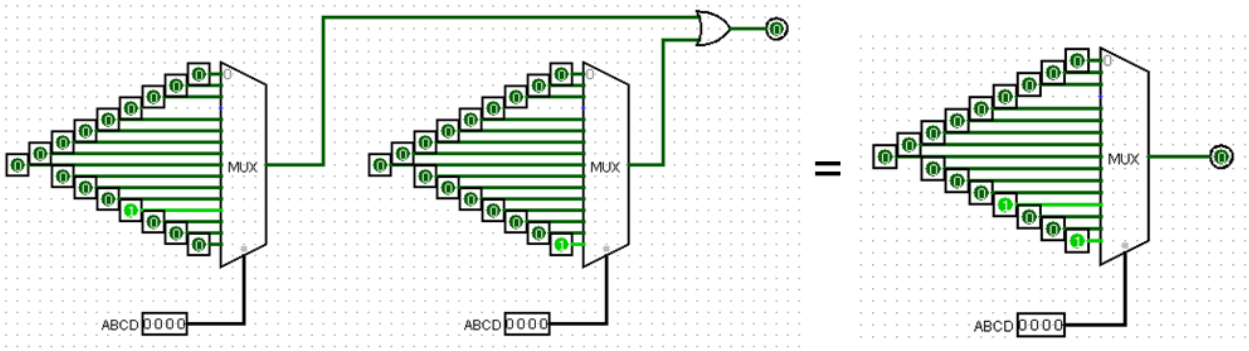

Figure 16. Circuits which do not leak feedback

However, even with only 4 binary inputs, that makes a more complex circuit with 16 possible states. What we saw earlier was that this complexity will quickly grow to a point where we cannot physically or practically implement it. Instead, it was more effective to allow feedback and use that same space more efficiently to increase the possible number of keys, which will benefit us more. For our system, with 16 possible keys, we can use equations from Gray Boxes section to say:

$$16 = n(k - 1) + 1, \; where \; k = 2 \rightarrow 16 = n(2 - 1) + 1 \rightarrow n = 15$$

This means if we want the same level of security that our four inputs with no feedback provide, in a system where the attacker can get perfect feedback, we need 15 inputs. This is still a simpler circuit than using the 16:1 multiplexer and provides much higher levels of security against brute force attacks or random guessing (32,768 keys vs 16). Of course, other techniques mentioned earlier for feedback obfuscation can be included to reduce the feedback.

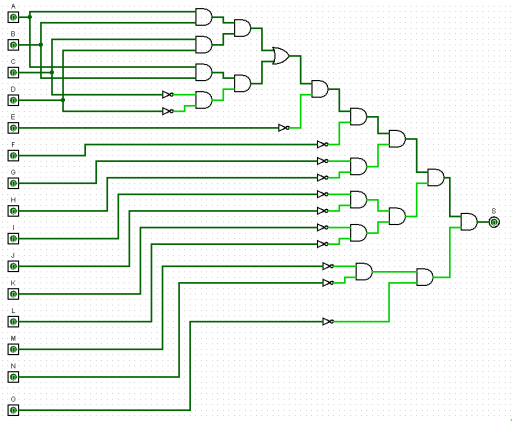

Figure 17. More Robust Circuit

Most standard pin tumblers and mechanical locks in general are not designed to support the kind of logic we have discussed so far. The systems typically compare individual tumblers, regardless of the adjacent tumblers position. In effect any combination of the true gates works and ordering does not matter. This means when we add an additional gate or master tumbler, we implement the following logic instead:

$$AB((C + \overline{C})(D + \overline{D})) = AB((1)(1)) = AB$$

$$AB \neq ABCD + AB\overline{CD}$$

This however is not equivalent to what we wrote before, and if we do the math, we see probability of access is greater when we compare individual tumblers, in this case, by a factor of two.

$$P_r(AB) = \frac{1}{2^2} = 0.250$$

$$P_r(ABCD + AB\overline{CD}) = \frac{1}{2^4} + \frac{1}{2^4} = 0.125$$

$$0.250 > 0.125,$$

This means that even though we only added one key to the system, instead of the attacker having twice the likelihood of getting access, the attacker has four times as many chances of opening it. This is without considering feedback, which further improves the odds for the attacker. In practical applications for mechanical locks, this typically occurs any time we have multiple keys which can be valid for a single common sheer line. In practice, if more additional keys are needed, one of

these existing possible keys should be used, rather than further reducing the security of the lock by adding additional gates or mastered tumblers.

The problems with master keying do not stop there. Typically, master keying is used to allow one master key to operate a larger set of locks, while the alternative (user, operator, change, servant, maid) keys only open a single lock (or a lower subset of locks). In cases where an attacker has one of the operator keys this can allow for privilege escalation attacks. Matt Blaze discusses how with one working key in a single sheer line master keying system, where $P_r = k^n$, the master key can be determined using n key blanks, in $n(k - 1)$ attempts [70]. Because the attacks only require testing a key, do not need to be done at one time, and do not require any special tooling or skill, it is very high risk. If there are multiple attackers each with unique operator keys, they can also share that information to reverse engineer the master key.

It is sometimes said that an operator key should never be able to be filed down to create a master key. That is based on the attack above, impressioning attacks, and the extreme weaknesses of warded lock designs. The concept that an absence of information should not lead to privilege escalation is very logical and should be followed. Filing a key is not actually providing less information though, it is providing information on a different keying. For restricted keys, where blanks are not commonly available, requiring a new key to manufacture a master key is very practical advice. However, for common key blanks an attacker could easily acquire, there is no significant benefit to requiring the attacker to purchase more blanks, but imposing a restriction as a policy could further inform the attacker of the possible keyspace, reducing the number of attempts needed.

One method to address the issues of unintentionally adding valid keys and privilege escalation is to use multiple independent cylinders, as discussed in later section 3.6 *Multiple Keys - Multiple Independent Locking Mechanisms*. This can be more costly requiring more components and space, so an alternative often used is multiple sheer lines. This is done with large format interchangeable core (LFIC) and small format interchangeable core (SFIC) and master ring systems [68, 69]. LFIC and SFIC use an operator key, which allows the lock to be opened, and a second sheer line for a control key, which allows the core to be removed for maintenance.

When properly implemented, there should only ever be one control key possible for an interchange core. When no further master keying is used, the two sheer lines can act like false gates for each other and increase the number of attempts needed to open the lock. At the same time, the lock can also be opened when the control key is used, so for an attacker simply looking to open the lock, picking to either control or operation is a success. We can estimate the maximum number of keys

an attacker needs to test to open the lock with perfect feedback, two sheer lines, two unique keys, and no additional false gates with the following equation:

$$Number\ of\ keys\ to\ test\ =\ \frac{n(n+1)(k-1)+2+k(n-1)n-n}{4}$$

If we plot this compared to an equivalently pinned core with a single key and sheer line, we see that the exact configuration of k and n determine if it would theoretically require more attempts to open. For a typical SFIC or LFIC cylinder, there are slightly more possible keys for the single sheer line case (~9%), but if we were to also account for increased test time of dealing with getting stuck in a false gate, it could make the total attack time longer with a cylinder with dual sheer lines. There is no significant difference in theory. In practical application, attacker skill sets with false gates will likely be a deciding factor and could easily make dual sheer lines the more difficult lock.

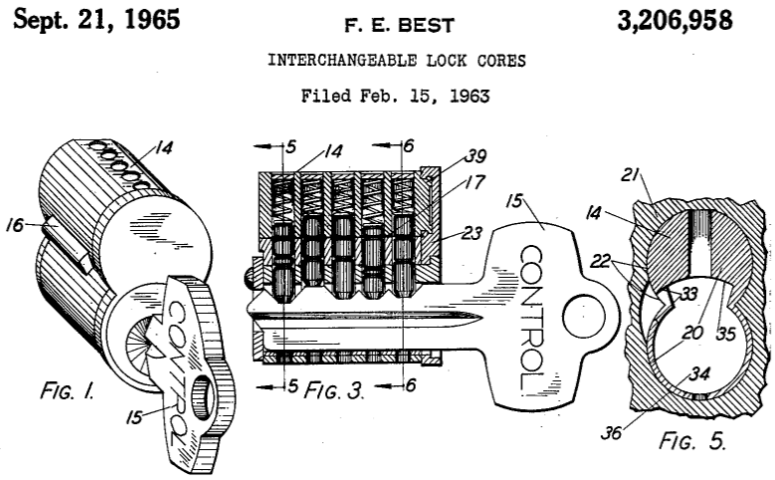

Figure 18. Interchangeable Core Patent

SFIC and LFIC locks can be further master keyed at the operator sheer line, which will reintroduce the myriads of problems mentioned earlier. Locks with master rings also use two sheer lines, but neither is for maintenance purposes, both are intended to open the lock. The Folger Adam model 110 mogul cylinder is an example of this used in detention facilities [68]. These will share similar characteristics to the SFIC and LFIC discussed above. One disadvantage of using multiple sheer lines is in reverse engineering [70]. If the locks can be taken apart, when there is one bitting per sleeve, and the master key read directly. If master keying on a single leave is used, there can be multiple configurations of the pins which would create a master key, so the attacker may still need to try multiple keys.

Master keying is an area electronic locks have large advantages. Software functions can easily be called iteratively through an array of hashed keys completely independent of each other. The array of secret keys can be buffered and results XORed like the example in section 2.4.4 to limit the information leaked on how many keys are in the system and their hash. While the same concept could be employed in mechanical systems, it would be much more costly and complex.

Lastly, it is worth warning about an alternative method called Maison keying. Maison keying allows multiple keys to access a shared lock by removing pins in the shared lock, such that the remaining ones match all keys. For example, a lodge might want to allow all guests to use the laundry, but only some to access the rooftop. To do this, pins are removed from locks used in common areas.

Location	Key Bitting	Number of Pins Used
Room A – VIP	178**161**	6
Room B - VIP	216**161**	6
Room C	8163**61**	6
Room D	3564**61**	6
Room E	9364**61**	6
Rooftop Lounge - VIP	###**161**	3
Shared Laundry Facilities	####**61**	2

Table 6. Maison Keying

This causes the number of unique keys possible for all locks, especially those in common areas, to be significantly reduced. By opening the locks in common areas, an attacker can also determine which portion of the keys are common for all rooms. Marc Tobias notes Maison keying weakens security so much that random keys for other systems may begin to work, and that in burglary investigations it should be determined if Maison keying was used [30]. Providing a second key which has access to common areas is preferred. This enhances common area security and prevents common area locks from leaking information on other keys.

3.5 Multiple Keys - Multiple Interdependent Locking Mechanisms

When two separate unique keys are required to access a system, the keys are normally issued to multiple people, and it is called a dual custody lock, or Two Person Integrity (TPI) System. These are often used for trust and liability purposes, such that one person cannot access or tamper with a system alone. These will be seen used for drop boxes, safety deposit boxes, classified information, weapons storage, or trapped key interlocks for industrial safety. It is interesting that these systems can also be seen in antique lever padlocks [63].

Figure 19. Dual Key Internal Locking Device (ILD) for weapons storage

Because two or more keys are required, the probability of access with random keys is:

$$where\ q\ =\ number\ of\ keys\ required$$

$$P_r = \frac{1}{qk^n}$$

$$if\ "q"\ different\ types\ of\ keys\ or\ locks\ are\ used,\ the\ likelihood\ will\ be:$$

$$P_r = \frac{1}{\sum_{i=1}^{q} k_i^{n_i}}$$

For an attacker with perfect feedback the odds will not increase significantly. It will be the equivalent of picking a single lock with additional tumblers.

$$When\ order\ of\ testing\ matters,\ P_f = \frac{1}{\frac{qn(qn+1)(k-1)}{2}+1}$$

$$When\ order\ of\ testing\ does\ not\ matter,\ P_f = \frac{1}{qn(k-1)+1}$$

In theory there are certainly designs possible that are so tightly coupled, that manipulation requires going back and forth between the two locking mechanisms simultaneously. In most mechanical systems though, the tolerances coupling with multiple locks will be much more loose than those preventing the lock from opening, so it will be possible to pick open one lock independent of the other and then pick the other lock to fully access the system. This does not

need to be the case though, for example, you could extend a single pin tumbler plug so that one key needs to be inserted on one end, and another key on the opposite end, and in the middle exists a notch for a ball bearing. Not high security by itself but does require the total number of pins to be picked at once, versus half at a time.

For dual custody systems where physical keys are not used, but instead a pin or a combination is entered, there is the risk the first user suddenly needs to leave after entering their pin or combination. This could allow the lock to be manipulated and opened easier by an attacker, or for the system to be tampered with by the second authorized user, while the first user is not present or aware. To prevent this, open windows can be added, such that the second combination or key must be entered in the time window, or the first key will need to be reentered. The Sargent and Greenleaf 2740 requires both combinations to be entered within two minutes of each other [62].

Exceptions do exist where two keys are expected to be used by a single user. For example, the double cylinder lock from JC-LOCK connects two keys and a knob together with a set of gears, such that when the knob is turned, both keys are turned at the same time. This category also applies to many forms of Two Factor Authentication (2FA) and Multifactor Authentication (MFA), where the key type is different, but the lock requires both to open. For example, some safes require the user to enter both a combination and provide a key.

Figure 20.
Two Cylinder Lock, Geared Key

Dual custody locks may not always offer the assumed level of security. While they increase tumbler complexity, skilled attackers can still manipulate them. If vulnerabilities like bumping exist, their security benefits become negligible. A dual custody system using standard tubular locks is less secure than one utilizing Medeco cores, which in turn is less secure than a system employing S&G 2937 Group 1 combination locks combined with time delays and controlled access windows. Dual custody is most effective when both locking mechanisms incorporate high-security designs; otherwise, for low-security locks, the benefit may be negligible.

3.6 Multiple Keys - Multiple Independent Locking Mechanisms

This category could apply to the locks discussed in section 3.3, *Single Keys - Multiple Independent Locking Mechanisms,* that have had master keying applied to them, as discussed in section 3.5 *Multiple Keys – Single Locking Mechanism*. To avoid being repetitive, we will not revisit those cases.

Instead, we will look at systems where unique keys and can be used with unique locks, to open a single system. These use “or” logic, internal lock one or two can grant access. Because they use “or” logic an attacker can choose the system with which they believe they have the best odds, or they may attack both and see which opens faster.

$$P_i$$

$$Attacking\ all\ at\ once,\ probability\ of\ access = P = \sum_{i=1}^{q} P_i = \sum_{i=1}^{q} \frac{1}{k_i^{n_i}}$$

Today, the most common application of this is probably providing a mechanical backup to an electronic system. Batteries can die, users can forget their pins, or electronics may be more prone to failure in certain environments. Mechanical locks provide a familiar backup that does not require power. This can certainly be a useful feature, but not normally be seen in high security systems. Lost power can mean losing some desired features, such as auditing. Instead of providing attackers with a method to bypass that with another locking mechanism, plugs may be provided to provide power from an external source should the internal power die. This does provide attackers with another interface with the lock and should be protected accordingly. Some combination locks, like the Kaba Mas X-10, have generators built into them, so they can be charged by turning the dial [65].

The risks of lost keys or pins is typically accepted in high security systems. Some consumers have been more upset to find out their device did have a “backup” or “backdoor” method for opening their device, as was the case with Liberty Safes with its “master reset codes” [66, 67]. Electronic hardware can be sourced and integrated into an enclosure to meet environmental conditions it will be used in with an acceptably low mean time between failures (MTBF). These systems are only as strong as the weakest lock. Very often in consumer devices, the backup lock is either a tubular or warded camlock. They are typically very low quality and can be opened in seconds, nearly as fast as having the real key.

There is another type we have not discussed, called Dual Entry or Dual Cylinder locks. These use two separate cylinders, either of which can result in the lock opening. The typical application for these is to allow a master key to be used without the security issues that come with master keying, or to allow keys from two different keying systems to be used to open a common lock [71].

4. Human Factors:

Humans are not deterministic and provide conditional security at best. For an access control system to be useful it must interact with humans, and at the time of writing, must still be designed by

humans. A high security system needs to account for human factors throughout the product life cycle. This means first knowing who you are designing for and what features need to be built in. The tables below can be referenced for brainstorming features, but some markets like hospitality and aerospace will have more nuanced requirements.

Importance of Features vs Market	Residential	Commercial	Industrial - Safety Critical	Finance -Banking	Government	Military
Ease of Use	High	High	Medium	Medium	Medium	High
Ease of Maintenance	High	Medium	Medium	Low	Medium	Medium
Ease of Rekeying	High	Medium	Medium	Low	Medium	Low
Destructive Resistance	Low	Medium	Medium	High	High	High
Nondestructive Resistance	Low	Medium	Medium	High	High	High
Mobile Apps -Monitor or Control	Medium	Medium	Low	Low	Low	Low
Alarms	Low	Medium	High	High	Medium	Medium
Tamper Detection	Low	Low	High	High	Medium	Medium
Modularity	High	High	Medium	Low	Medium	Medium
Reliability - MTBF	Medium	Medium	High	High	Medium	High
Standards Compliance	Low	Medium	High	High	High	High

Table 7. Feature Important by Market

In addition to understanding what consumers want, it is also important to know what other systems are currently available. There is a massive number of products, it will be a very rare use case that cannot be covered by some combination of products available; not that they cannot be improved. Many are low security with severe vulnerabilities but are at a low cost and targeted for use on products consumers are willing to take those risks with (gym and school lockers, sheds, garages). Many well-designed high security solutions also exist you can reference for inspiration, and to see what is already patented. Searching YouTube for these locks can provide further insight into how well these locks really resist attack in lab or controlled settings, and what consumers really think of them.

Disclaimer: The following table does not endorse any locks or brands for a specific market, purpose, or feature. Some of the locks listed have major vulnerabilities, and many other brands and models are not included. This table is intended only as a quick reference for locks and brands commonly found in different markets. Availability and popularity may vary significantly by region.

Lock Type	Residential	Commercial	Industrial - Safety Critical	Finance - Banking	Government	Military
Padlocks	ACE, Abus, Master, Brinks, Squire	Lockwood, American, Master ProSeries	PACLOCK 90A Pro, Knox, S&G 881, Abloy PL 330	Abloy PL 975, PL 362, EVVA MCS, 4KS	PACLOCK RD 656, Abloy 658, S&G 8077	S&G 951, 833C
Cylinders	Yale, Schlage, Kwikset, Phillips	SFIC & LFIC, ACE Tubular, Everest, Mul-T-Lock	PACLOCK PR1, Medeco, Abloy Classic, EVVA 4KS	Robur 2391, BiLock, Abloy Protec2, Mul-T-Lock	Medeco R1, S&G 8430, BiLock	Medeco D4
Safes	Sentry Fire/Water, Fort Knox, Liberty	Knox Box, Honeywell 5912, Protex drop boxes	KL Security TL-15 safes, T2 Magazines, Knox MedVault	S&G 6370, LeGault, LaGard 3330, Diebold	GSA Class 5, Kaba Mas X-10, S&G 2740B	Class 5A, S&G 2937, ILD

Table 8. Locks used in various markets

I would like to take a moment to commend The Pacific Lock Company (PACLOCK) for adopting a refreshingly different approach compared to most lock manufacturers by actively engaging with the locksport community. As part of this engagement, they have distributed '200K Club' patches and stickers to individuals who successfully and publicly demonstrated their ability to pick open their 90A Pro series lock. While this initiative doesn't inherently improve the baseline security of their products, it does promote transparency and honesty about the true level of security provided. Industry and consumers could benefit from more collaboration like this in the future, between manufacturers, security professionals, and the locksport community.

4.1 Research and Development:

To build any system, it is crucial to understand its possibilities and limitations. By analyzing the history of locks and breaking them down into simple components, we can infer the fundamental limits of both offense and defense. We can use this information to make estimates of how long an attacker with perfect information and flawless execution would need to breach a lock. This is part of identifying failure modes. In assessing failure modes, we consider several factors:

- **Severity**: How compromised is the system? Who or what is at risk? Could this result in bodily harm?
- **Likelihood**: Is the failure less probable than a lightning strike? Or is it a scenario likely to occur during normal use and maintenance?

This information is often organized with tools like a Risk Assessment Matrix or a Failure Modes, Effects, and Criticality Analysis (FMECA). These documents serve as references for stakeholders—engineers, managers, investors, operators, and clients—to determine whether risks are acceptable or if additional controls are necessary. Importantly, risk assessments evolve cyclically with each design iteration. The considerations for a lock used in an indoor gym locker differ significantly from those for securing industrial chemicals in a jungle climate.

Risk assessments often rely on educated estimates, which is acceptable if the estimates are well-informed. However, all too often, we encounter new locks on the market advertised with labels such as "High Security," "Maximum Security," or "Pick Proof." Despite these claims, such locks are frequently breached within seconds. While many of these labels are meaningless marketing buzzwords, some designers genuinely aim to create high-security systems but fall short due to limited knowledge of attack methods.

This lack of expertise becomes evident in design drawings. Some designers, unaware of common and advanced techniques for breaching locks, attempt to innovate without understanding fundamental attack methods. These include techniques like picking, zipping, raking, rocking, float picking, jiggle testing, bumping/rapping, overlifting, impressioning, molding, manipulation, decoding, slamming, and bypassing.

Lock enthusiasts focusing solely on manipulation techniques might miss the forest for the trees. Statistically, most attackers will not try to manipulate a lock to gain access. For those that do, they will not have “perfect” feedback. Every lock picker, cracker, or impressioner makes mistakes and experiences inefficiencies. Attackers may also find the fear of being caught releasing some adrenaline, causing “tunnel vision” and reduced fine motor control. Sweat can make tools slip, and the need to remain unnoticed may force attackers to work in dark or awkward positions. This

further reduces their situational awareness and ability to manipulate the lock without making mistakes. Many attackers may also be uninformed opportunists, utilizing basic attacks, and hoping for the best. In these cases, trick locks (a little layer of security through obscurity) can prove to be very effective against an unskilled attacker.

While all this might be acceptable for low-security applications, safety-critical systems demand greater rigor. Subject matter experts should be involved early in the design stage to ensure that the lock meets its security goals and provide informed estimates for severity and likelihood. This is not to stifle innovation but to advocate for collaboration with the security community familiar with the application. Flaws are least costly to address during the design phase, where they can be identified and mitigated before production.

Beyond design flaws, another common pitfall arises when security components are outsourced to the lowest bidder. Once again, quality requirements depend on the application, but we often see devices in medical and firearms storage, where what might be an acceptable electronic security system is bypassable via a $5 backup tubular lock or $1 wafer lock. Getting SMEs familiar with attack and penetration testing in the design and early review process will help catch these liabilities.

4.2 Implementation and Validation:

> *"In respect to lock-making, there can scarcely be such a thing as dishonesty of intention: the inventor produces a lock which he honestly thinks will possess such and such qualities; and he declares his belief to the world. If others differ from him in opinion concerning those qualities, it is open to them to say so; and the discussion, truthfully conducted, must lead to public advantage: the discussion stimulates curiosity, and the curiosity stimulates invention."* A.C. Hobbs, Rudimentary Treatise on the Construction of Locks, 1853 [82]

> *"We tend to put a lot of weight on what something is designed to do and ignore what it actually can do, and this is really important, because the delta between those two concepts is the attackers playground."* LockPickingLawyer, SaintCon, 2021 [61]

Even for a good design, mistakes are made in implementation. The programmer thought their software said *while(isValid == true)*, but what they actually said was *while(isValid = true)*, and instead of testing for validity, ended up setting validity. In-house unit tests to verify early implementations and inspection of prototypes allows these to be caught before they become costly manufacturing defects, recalls, or lawsuits.

For high security systems, third party inspection and classification will typically be necessary. Insurance companies will require minimum levels of security to be in place to provide certain coverage [29]. Per DoD 5200.18, the General Services Administration (GSA) is responsible for establishing the requirements needed for access control systems, which must be followed by government agencies or any third party working for the U.S. Government storing classified information [30]. FP-L-2740 and AA-F-358G are standards used by the Federal Government for evaluating containers and locks for safes, security filing cabinets, and vault doors [30]. Regulatory and standardization agencies and boards across the world exist for the purpose of certifying the level of security provided by access control systems [20], [30], [31], [41], [42].

Location	Organization	Standard	Notes
Australia	CSA	AS 4145	Cylinder locks
Europe	CEN	EN 1047, 1143-1, 1143-2, 1300, 12209, 14450	high-security locks, safes, deposit systems, data rooms
France	CNPP	A2P Rating System	1-3 Stars rating system
Germany	DIN	18251, 18252, 12209	Cylinder locks, hardware
Japan	JIS	A-1541, S-1037	Locks and Latches, Fire Safes
Netherlands	SKG IKOB	NEN EN 14846, 12209, 1303, 15684, 16864, BRL 3104	Mechanical, Electric Locks, Padlocks, Burglary Resistance
United Kingdom	BSI	BS 3621, 7950, 8220, 8621 BS EN 1300, 1303 1906, 1935, 12320	Cylinder locks, thief resistant, high security, cylinder locks, lever handles, hinges, padlocks
United Kingdom	LPCB	LPS 1242, LPS 1175	Cylinders and enclosures
United States	ANSI	156.2, 156.5, 156.13, 156.23, 156.25, 156.30, 156.50	Locks and Latches, alarms, high security locks, electronic locks
United States	ASTM	F883, D3580, G85, G112-92	Padlocks Environmental Effects
United States	GSA	AA-F-358G, FF-L-2740B	Containers and safes
United States	UL	72, 140, 294, 437, 608, 639, 687, 768, 786, 887, 2058	Fire resistance, key, combo, time, and high sec locks, alarms
United States	DOD	MIL-STD-810E, MIL-P-43607G, DOD 5100.76	Environmental, Unauthorized entry (surreptitious and forced)
International	LPU	Belt Ranking System	Locksport, Hobby Classification

Table 9. Common Standards Used to Evaluate Locks

The Manipulation Resistance Estimate Guide at the end of this paper is provided for reference as an example of a standard which is not dependent on tester skill in manipulation to evaluate the level of security a system provides. While the methods and criteria used in some of these standards are a point of contention in the security community, getting classifications from these various standards helps keep industry honest, and consumers properly informed.

That being said, standards also have limitations. Marc Tobias, who served for over 15 years on the Underwriter Laboratory (UL) Standards Technical Panel on locks and safes, said "*Compliance-based security, unfortunately, rarely identifies security issues. Attacks that aren't foreseen can't be prevented. If not envisioned within the standards, such attacks can't be tested against, predicted, or prevented.* [78]" He further suggests creating a Vulnerability Assessment (VA) plan and team, separate from the design engineers, specifically to find vulnerabilities and score them against a 3T2R (Time, Tools, Training, Reliability, Repeatability) system [78].

Lastly there are massive hacker and locksport communities that have a real passion and love for trying to manipulate access control systems and pick challenge locks. Many are willing to test systems freely, provide feedback, and some will even agree to sign Non-Disclosure Agreements (NDA) while the initial design and implementation has the bugs worked out, or to work on contract. Do not be afraid to reach out to them early, as many of them will be the same people testing your system when it is out for sale, and for better or worse, they will be sharing their thoughts on the final products you have invested heavily in.

4.3 Distribution and Deployment:

Currently many locks purchased at local hardware and department stores have keys visible in the package, or key-bitting labeled on the side. This helps contractors purchase locks with the same keying, but it also means attackers can know a person's key by watching their purchases at a store.

To ensure keys remain secret, and that an access control system has not been tampered with (such as installing malicious software), we want to minimize third party access between manufacturing and consumers. This can be done by first shipping the key with a random code directly from the manufacturer in a tamper sealed container. The manufacturer notifies the consumer of the tracking information for the key. When the consumer receives the key, they confirm the tracking information. They then confirm receipt of their key by sending the manufacturer back the random code. The manufacturer can then send the access control system separately, also in a tamper sealed container with tracking information. This is to prevent tampering with either the initial key shipment, or the access control system using the key. In the past Purism has offered a customizable anti-interdiction shipping service for their electronic key tokens with most of these options available [24].

The USPS offers Registered Mail services which provide tracking, chain of custody records, stores mail in locked containers during transit and require signature upon delivery [22]. Should more assurances be needed, such as shipping a physical key currently in use, UPS offers an Express Critical Secure service which can include additional live tracking information, armored transport, and 24 hour screened escorts [23]. Other specialty-freight carriers may offer similar services.

Systems which allow users to change keys on their own once the access control system is received offer another layer of protection. The consumer can change keys upon receipt to reduce the risk of key leakage from either the manufacturer or shippers.

4.4 Usage and Maintenance:

There have been many cases where attacks were successful because default pins were not changed on access control systems. This has ranged from network routers to ATM configuration panels. It is a good practice to create a system which either uses a random factory key or requires the user to enter a new key upon receipt to prevent this.

For a high security system, which properly implements good design principles, it quickly becomes more attractive to steal a key from the user, then attempt to decipher one. The original time locks were built to prevent robbers from forcing bank managers to open vaults in the middle of the night. Today we see social engineering attacks like phishing constantly being used because of their relative low risk high payout potential. Multifactor authentication and one-time passwords provide damage control for these types of attacks.

Multifactor authentication requires a user to provide two or more forms of authentication. One is typically hardware based (a physical key, RSA token, YubiKey, Librem Key, a badge, a cellular phone, etc..) and one is typically information based (a combination, password, code word, pin, etc..). The forms of authentication are independent of each other, such that one cannot be deduced from the other. It does not enhance the security of the system as much as it limits damage of key leakage. When a man in the middle attack, keylogger, phishing website, or shoulder surfer successfully sniffs the password/pin, they still do not have enough information to access the system. In the case where text messages, push notifications, and emails are sent to the user requesting the secondary authentication this can also notify the authorized user an attack is occurring.

One-time passwords, or tokens, are electronically generated keys that can also provide damage control for key interception. This is also important for wireless systems to prevent replay attacks, where a key may be intercepted surreptitiously and later reused. Hash Based Message Authentication Code (HMAC) One-Time Passwords (HOTP) iteratively generate passwords which can only be used one time. If an HOTP is intercepted an attacker may use it once, if the authorized user has not used it first. Once the attacker has used it, this can also be an indicator to the authorized user that the system was compromised. Time-Based One-Time passwords (TOTP) iteratively generate passwords which can only be used in a given time window (often 60 seconds) before they expire. If a TOTP is intercepted, there is a very narrow range the attacker must make use of it. At their root, HOTP and TOTP still rely on the secrecy of their root key, or seed. If the seed is

compromised, all generated keys are compromised. Email and SMS messages are typically unencrypted and more vulnerable to interception, so locally generated passwords (either via app or hardware token) are preferred. Push notifications may be encrypted and used to securely transmit tokens remotely, but this is application dependent and should not be assumed to be the case. The use of securely generated tokens also reduces risk to a user choosing or reusing common passwords or pins.

Another important part of maintaining an access control system is the ability to remove expired keys and generate new ones internally. This zero-trust practice allows a user to generate a key no other user is aware of, reducing the likelihood of it being leaked or misused by a third party. The Kwikset's SmartKey is an example of technology allowing users to easily rekey a mechanical lock on their own with no training required. This system is not high security and has some significant weaknesses regarding decoding, but the ability to quickly change keys can be especially useful when considering insider threats or leaked keys. The ease with which it allows a key change is commendable.

4.5 Vulnerability Disclosure Programs:

"*Plans are useless, but planning is indispensable.*" – Dwight Eisenhower

History has shown that even high-security locks, despite years of rigorous testing and a strong pedigree, can still be found vulnerable after deployment. Advances in tools, techniques, and research continuously reveal new weaknesses. To effectively handle these potential security risks, companies must establish a clear plan before they occur. This is typically done through a Responsible Disclosure Policy (RDP) or a Vulnerability Disclosure Program (VDP).

Without such a program, poor communication can lead to increased legal liabilities for both the company and researchers, accidental exposure of additional security weaknesses, and a higher risk of uncoordinated disclosure. On the other hand, a well-structured disclosure program fosters trust, encourages responsible reporting, provides legal protection, and helps safeguard both businesses and the public from security threats.

When developing these plans, they can generally be broken down into four broad stages:

1. Acknowledgement – Confirm receipt of the disclosure to the reporter and provide a tracking number with an estimated timeline for further responses.
2. Triage – Assess the validity of the report, determine whether the vulnerability is new or already known, and classify its severity and likelihood. The classification system should be defined in advance.

3. Remediation – Determine and execute appropriate corrective actions based on the classification. Responses may range from no action to a full-scale recall and public statement.
4. Disclosure – Once remediation is complete, publicly acknowledge the vulnerability and the researcher who discovered it (if they wish to be credited).

The exact policies and procedures will vary by industry, company, and product, making this process non-trivial. Some organizations, such as HackerOne, provide vulnerability disclosure management as a service [77]. At the time of writing, Schlage, an Allegion company, was using HackerOne to power their Vulnerability Disclosure service [79].

Additionally, Marc Tobias, a security researcher and lawyer, extensively covers the legal and regulatory considerations for locks, safes, and security systems in *On Locks and Insecurity Engineering* [78]. His work includes guidance on ethically handling defects and disclosures while minimizing liability exposure.

4.6 Decommissioning and Disposal:

For accessing electronic systems, one of the easiest tried and true methods to determine a key is to find a previously used key that is not well secured and begin trying variations on it. People reuse passwords, and pins, and slightly modify them for the security requirements of their organization. Looking at over 3 million four-digit pin codes released from data breaches, researchers found 20 pins made up 27% of the pins used [75]. When a heat map is made to display the distribution of pins usage, we can quickly see it is not uniform and concentrates around dates and repeating numbers. Attackers have long understood this and will try to gather information on their targets to orient where they need to concentrate their efforts. For example, Prioritize is a python script that can be used to generate permutations according to a list of prioritized keys, allowing attacks to concentrate in these high usage zones, and reduce brute force attack time [32]. It has also been estimated that the average person will reuse a password 14 times, with 49% of employees simply changing a character on their password when required to update every 90 days [76].

The US DoD Manual 5200.01 Volume 3 states all combination padlocks and safes can be disposed of non-destructively, after the combinations have been reset to the default values of 10-20-30 and 50-25-50 respectively [80]. DoD Manual 5100.76 states "*Unserviceable high-security padlocks, keys, and cylinders shall be controlled until properly destroyed.*" [81] Destruction is an important step to prevent attackers from being able to get or make working key copies for these restricted locks. The keying can be reverse engineered by picking the lock, and milling machines do exist which can make copies of the restricted keys used by the military. Of course, if a single key and padlock were

disposed of non-destructively but were part of a larger keyed alike system still in use, this would be an even larger security risk.

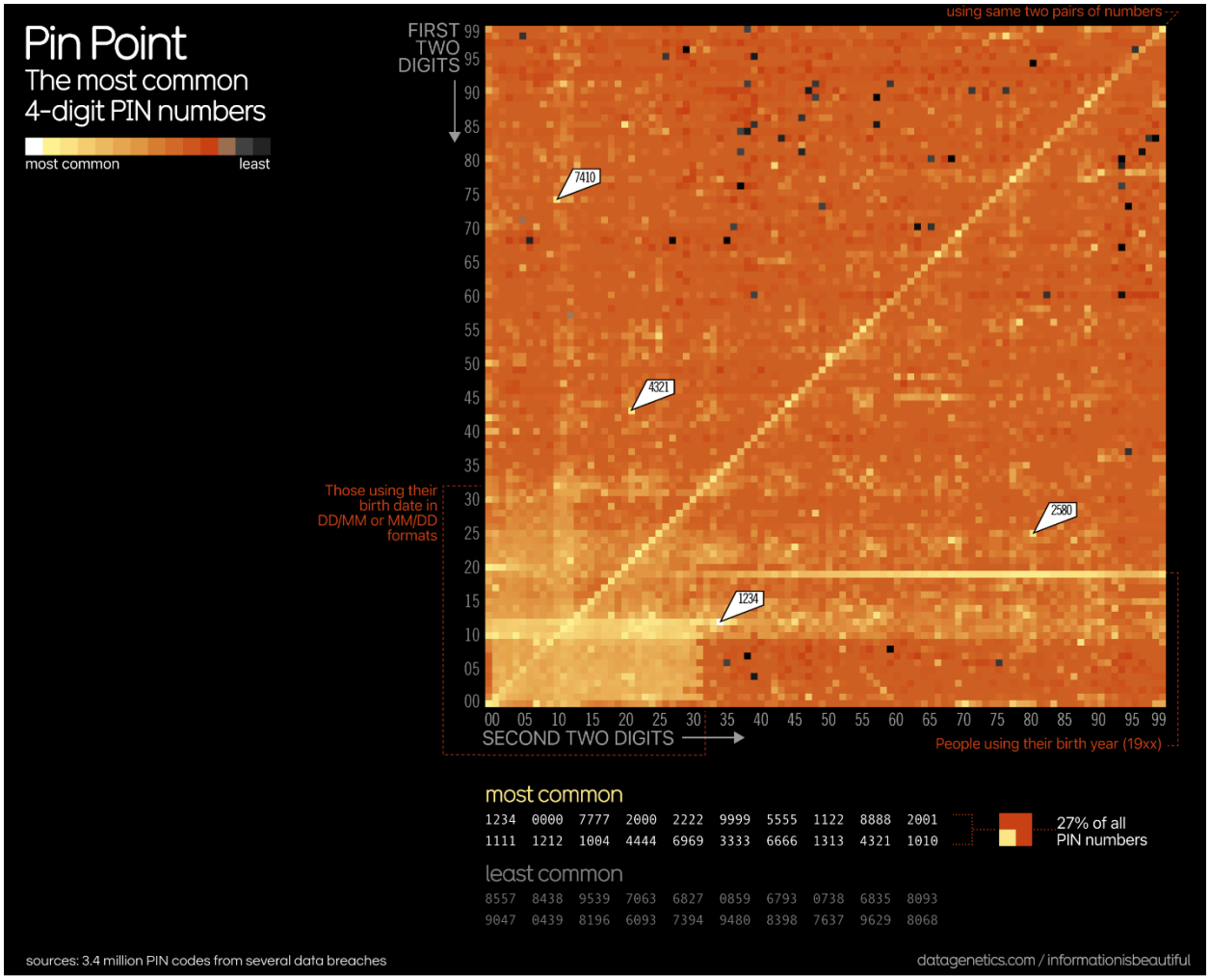

Figure 21. Commonly used pins, Courtesy of http://informationisbeautiful.net/

When equipment is disposed of, sanitizing all data and keys will reduce the likelihood an attacker can reuse this information. Establishing expirations on keys can also reduce the likelihood of an attacker using keys from disposed, recycled, or forgotten equipment. Ideally when a user no longer requires access to a system, their key is removed from the system rather than reissued to another user. When updating a password, a similarity check can also be used to prevent password reuse. The password can normally be hashed for security, but when it comes time to reset the password, the system asks for the users current existing password. When it is confirmed that the entered password is correct, the plain text version of it can be compared against the plain text of the new password for similarity. This has limitations in only comparing the last password (a user could alternate between their top three), but saving password histories can introduce more risk by providing a target for attackers. Even if an expired password is not of use on one system,

there is a strong statistical chance the attacker could use the password (or close form of it) on another system the user has access to, or that they can determine a pattern the user has for creating new passwords.

Also note, one of the methods for attackers to learn about a system is through acquiring ones being disposed of and recycled. When equipment is disposed of, it provides attackers with a platform they can test on remotely without concern for detection. Decommissioned safes, ATMs, safety deposit boxes, and government containers can often be found at relatively low cost in secondary markets and used for testing and training. This becomes more of a risk when standard default or master keys are used (ex: hotel safes with mechanical master key overrides). There may be cases where leasing the access control system is more appropriate for manufacturers and consumers.

Figure 22. Access Control Devices Recently Sold Online

In the figure above you can see some items recently sold on Ebay. Specifically, a Hotel Safe w/ Backup Master Key, Police Patrol Gun Rack, Apartment Mailbox, ATM, GSA Cabinet Safe, MedVault, Laptop with what appears to be a user account still active, and Knox Box. While there are certainly legitimate reasons for making any of these purchases, each one could also be of benefit to different profiles of attackers. Further searching can quickly reveal cases which also appear to violate DoD Manual 5100.76.

When a program or unit shuts down, security considerations in equipment disposal can be overlooked, especially in cases of unplanned shutdowns. Typically, management is responsible for deciding how equipment is handled, and in some instances, they may prioritize financial incentives over long-term security risks. To mitigate this, organizations can lease critical security equipment rather than own it outright, ensuring that proper disposal procedures are followed.

Ultimately, one man's trash can be another man's treasure—but in security, one organization's discarded assets can become an attacker's greatest asset. Establishing clear policies for key expiration and secure disposal can significantly reduce the likelihood of security breaches.

5. Physical Strength – The Gordian Knot:

In 333 BC Alexander the Great entered his army into the capital of Gordium, where there was an oxcart with an intricately tied knot of cornel bark securing the yolk [46,47]. It had been prophesized that whoever could untie the knot was destined to rule Asia. When Alexander went to the cart, it was expected he would have to tediously unravel and decode the knot, but as the story goes, after accessing the knot, he drew his sword and cut it off.

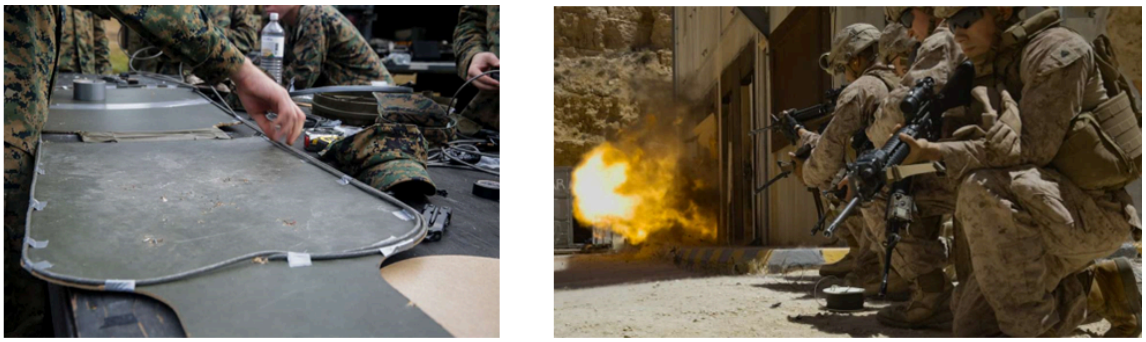

Figure 23. DOD Public Domain,
Left: US Marines prepare an oval charge for creating doors in walls and ceilings.
Right, US Marines train for urban breaching with explosive charges

In this paper we primarily look at manipulation resistance (remember it is lockpicker perspectives), but typically criminal activity will involve “cutting the knot” or looking for where there is no knot at all. The public statistics on surreptitious or covert entry as opposed to forcible entry in crime are fairly limited in detail [48, 49]. We can see in a 2003-2007 U.S. Department of Justice report of the average annual burglaries completed, 44.1% damaged or removed a door or window, 33.5% of entry was through an open or unlocked door or window, and 2.1% involved picking a lock [49]. There are additional categories which are certainly related, such as had key (3.8%), or entry through locked door by unknown means (2.4%), but without more information, it's limited what we can infer about these entries [49]. Whether forcible or non-forcible entry leads also appears to vary year by year [48, 49]. The statistics do tell us that we 1) need to ensure we use the access control systems we make by securely locking them, and 2) we need to ensure they are resistant to physical attacks.

Trapped key interlocking can be used to ensure locks are engaged, by requiring a user first engage a lock to remove their key and requiring the same key be used to access another door. This is common in safety critical industrial power lock out systems. Man traps, revolving doors, airlocks, and full height turnstiles can all be used to ensure a door is always secured and prevent tailgating or piggybacking. Be aware, Americans with Disabilities Act (ADA) compliant turnstiles, or ones equipped with panic or crash bars are often easily bypassed with an under the tool, double door tool (DDT), or equivalent device. Request to Exit (REX) sensors can also be a weak point and be bypassed via movement or compressed gas [53]. If such automation is present, ensuring doors are well sealed when closed (snug fit plus rubber molding and door shoes) and sensors are properly calibrated (not overly sensitive) can help prevent bypass [52]. Alarms triggered when locks are not secured within expected times, and security policies to check doors/locks are secured will assist.

The physical security of the system is going to have massive variations in design considerations depending on what resource is being secured. It may be a residential safe with high value heirlooms, a biosafety level 4 (BSL-4) laboratory for lethal airborne agents, or an Intelligence, Surveillance, and Reconnaissance (ISR) drone operating in a hostile country. For this paper we will have to keep it simple and generic.

For all access control systems there are a few good design rules. Use high-strength materials like hardened steel and stainless steel. Generally speaking; plastics, aluminum, and cast iron will not be appropriate enclosures for safety critical access control. Minimize the joints and interfaces in the exterior frame of the system. These provide locations for feedback to be emitted, tools to be inserted, and physically weaken the structure. Where there are joints, use guards to cover the joint and prevent easy insertion of tools. If mounting holes are predrilled, provide a method to securely seal them if they are not used. All hinges should be interior/hidden. The system should not be able to be dismantled for maintenance or repair unless an authorized key is provided. Security screws are a deterrent, but not a high security feature by themselves. Increasing the number of multi-point bolts securing access doors/panels will improve the strength of the door. The locking mechanism should be reinforced into the frame such that it cannot be easily pried out or pushed in with tooling.

Below is a list of common destructive attacks and respective countermeasures [20, 30, 50, 51, 74].

Destructive Attack	Susceptible to Attack	Countermeasures
Slamming, Dropping	Wood, Plastic Containers, Spring Loaded Bolts	High-strength metals, Deadbolts (not spring-loaded latches)
Kicking In Door	Wood & Fiberglass Doors, Thin Metal Doors, Doors with single Latch Bolt	Deeper screws on strike plate, Door reinforcer plate, Deadbolts, Reinforce Hinge

Screwdriver	Wafer Locks, Windows, Plastic Housings	High-strength metals, Steel components and housing
Hammer	Padlocks, Cast Iron, Windows, Exposed Hinges, Door Frames	High-strength metals, Steel components and housing, Door reinforcer plate
Hand Saw	Deadbolts, Padlocks, Chains	High-strength metals components and housing, Stainless Steel or Ceramic Pins
Wrenches, Pliers	Padlocks, Euro Profile Locks	Padlocks with ball bearings and shackle guards, Anti-snap reinforcement
Bolt Cutters	Exposed Chains and Shackles	Shackle Guards, High-strength metals, Hardened Steel, Chain/Shack Thickness
Chisel	Exposed Hinges, Cast Iron housing and bolt, Wood Door Frames	Concealed hinges, High-strength metals, Door reinforcer plate, Deadbolts
Nail Punch, Hinge Pin Removal Tool	Exposed Hinges	Concealed hinges
Prybar, Crowbar, hooligan tool, Hand Wedge Tool	Wood & Fiberglass Doors, Thin Metal Doors, Doors with single Latch Bolt	Door reinforcer plate, Metal Doors, Deadbolts, Locking Bars, Multi-point locks
Nail Puller, Dent Puller, Slam Hammer	Cylinder locks	High-strength metal components, Anti-snap reinforcement, Sacrificial breakaway face
Sledgehammer, Ram	Wood & Fiberglass Doors, Thin Metal Doors	Reinforced Hinges, Door reinforcer plate, Locking Bars, Multi-point locks, Steel security doors
Drill	Cylinder locks, Safes	High-strength metals, Mangalloy hard plate*, free spinning discs or ball bearings, stainless steel pins, Al2O3 chips***, bolt relockers, Bitumen layers
Grinder, Disc Cutter	Hinges, Chains, Shackles, Bolts, Thin Plate Safe Walls	High-strength metals, Ceramic Rods, Concealed hinges, Bitumen Layers
Hydraulic Press. Jam Spreader	Wood & Fiberglass Doors, Thin Metal Doors	Locking Bars, Multi-point locks, Steel security doors
Shotgun, Firearms	Hinges, Strike Plate/Door Jamb, Padlocks, Cylinder Locks	Reinforced Hinges, Door reinforcer plate, multi-point locks, Steel security doors, High-strength metal components
Low Explosives (Mapp Gass, Propane, Gunpowder)	Thin Metal Hinges, Bolts	High-strength metal components, Reinforced Hinges, Locking Bars, Multi-point locks, Safe/bolt relockers
Gallium	Aluminum and Zinc based alloys (Corrosion Resistant)	Avoid use of Aluminum and Zinc based alloys
Thermite	Thin Metal Safe Walls	Increase Thermal mass/Wall thickness, Ceramic Insulation, Safe/bolt relockers

Freon, Liquid Nitrogen	Cast Iron, Carbon Steel	Stainless Steel, Increase Thermal mass/Wall thickness, Safe/bolt relockers, chrome and nickel hardeners
Oxyacetylene Torch, Thermal Lance	Reinforced Steel Doors, Vaults, Armored Vehicles	Increase Thermal mass/Wall thickness, Laminated hard plate, Cu to Al walls**, Ceramic Coatings, Safe/bolt relockers
High Explosives (PETN, RDX, TNT)	Reinforced Steel Doors, Vaults, Armored Vehicles	Increase Wall thickness, Safe/bolt relockers, Reactive Armor

Table 10. Common Destructive Attacks and Defenses

* Mangalloy hard plate on the interior walls of a safe rather than exterior can be cheaper, allow the additional layers to help prevent delamination attacks, and further restrict access with hand tools [74].
** In a thermal attack Copper provides thermal insulation for exterior layers. If aluminum is used as the next internal layer, when the copper is hot enough to melt pressurized jets of vaporized aluminum can be expelled toward the attacker. The backblast of aluminum can deposit on tools and is unpleasant for the attacker [74].
*** Chips can deflect drilling, so placement towards the lock face can have greater impact [74].

The effectiveness of attack tools, such as lockpicks, drills, and even brute-force implements, depends heavily on the skill and experience of the operator. In many cases, non-intuitive techniques with basic tools can yield superior results. For instance, instead of applying excessive torque to a screwdriver to shear lock components in one motion, attackers may use a rocking motion to gradually grind down tumblers. Similarly, using multiple wrenches to apply force strategically can provide sufficient leverage to pry open padlocks with minimal effort. Proper tool selection also plays a critical role; choosing the correct drill bit for specific metals can mean the difference between snapping multiple bits or smoothly cutting through hardened materials. Even high explosives, when applied correctly, can be tailored for either cutting or pushing effects, producing vastly different outcomes depending on the target material.

Ideally, testers evaluating security systems should be well-versed in the nuances of these attack methods. They should also be given the freedom to implement hybrid techniques—combining multiple attack vectors where appropriate—rather than being restricted to conventional testing procedures. This approach ensures a more realistic assessment of a system's vulnerabilities, mirroring the adaptive nature of real-world adversaries.

6. Conclusion:

This paper has explored both the theoretical and practical aspects of high-security access control systems, focusing on the role of feedback, probabilistic security, manipulation resistance, and human factors that influence design and implementation. Additionally, it has examined physical considerations in lock construction and security effectiveness.

Key Takeaways:

- Access Control Security is Probabilistic, Not Absolute
    - Locks function as probabilistic security systems.
    - Security can and should be measured in quantifiable terms, allowing for objective evaluations of lock effectiveness. In many cases, we have mathematical models that can help estimate security levels.
- Common Weaknesses in Locks
    - Failure to implement zero trust principles.
    - Leaking useful feedback, which reduces attack difficulty from an exponential to a linear problem.
    - Lack of independent reviews and rigorous testing during early design and prototyping phases.
- Layered defenses reduce the probability of unauthorized access
    - Security can be significantly improved through layered defenses, such as:
        - Restricted access, time delays, staging, interlocking, false gates, buffering, hashing, redundant locking mechanisms, MFA, TOTPs, tamper seals, alarms, and relockers.
    - These measures help control attack time, mitigate feedback leaks, and minimize damage from security breaches.
- Security Thrives Through Transparency and Collaboration
    - Security should not rely on obscurity, as history has proven that such approaches fail in the long run.
    - Stronger security emerges through collaboration between manufacturers, security professionals, academic researchers, and hacker/locksport communities.

As attack techniques continue to evolve, some primary tools for improving security are:

- Security education
- Innovative design
- Robust independent testing

Rather than denying vulnerabilities or dismissing real-world attacks, the industry must embrace evidence-based security improvements to build more resilient access control systems.

By recognizing locks as probabilistic security systems, mitigating feedback leaks, implementing layered defenses, and fostering collaboration, we can design access control systems that remain resilient against evolving attack methods well into the future.

I hope this document will prove to be a helpful resource in the design of those future high security access control systems.

7. Future Work:

> "*The construction of Locks, is a subject on which many ingenious mechanics have employed their thoughts; and the art has received many and great improvements from their labours."* Joseph Bramah, A Dissertation on the Construction of Locks, 1785 [21]

For this paper to be accurate, relevant, and useful revisions will be needed. Those revisions are welcome! If there is a section in this document you find is inaccurate, misleading, or missing, please reach out to the authors. If inclined, you are also welcome to consider authoring the revisions or new sections yourself. Looking forward, below are some topics which could warrant future research and development.

1. Advancements in Staging and Interlocking Mechanisms**:**
    - Design of cost-effective solutions that integrate these features could provide much higher security locks in residential and common commercial applications.
2. Integration of Artificial Intelligence (AI) in Access Control:
    - AI processes massive data in real time for classification. Soon it may verify users, identify attackers, and limit or generate false feedback. A common concern is determinism and explainability, and that could apply in access control too.
3. Biometric and Behavioral Authentication:
    - We are seeing more commercial solutions with fingerprint scanners, facial recognition, and iris scanners. In the future continuous behavior authentication may be able to couple with biometrics for a new form of multifactor authentication.
4. Wireless Access Control:
    - Wireless Access Control provides a unique combination of exposed messaging with sealed interfaces. It may be good to explore how when combined with IOT devices we can have multiple users or roles in close proximity to each other with immediate access to various resources, and what the effects of such systems could be.
5. Sustainability and Environmental Impact:

- What can we do to reduce waste in the product life cycle of locks? How can we reuse keys, locks, and enclosures? How could modular and rekeyable systems enable this? Is leasing, buy backs, or returns viable?

6. Standardization and Collaboration:
    - Standards for qualification testing may be improved ensuring they are current with the latest attack methods. Tests based on lock characteristics could be more deterministic than ones performed by persons with varying skill levels.
7. Resilience Against Emerging Threats:
    - What role will quantum computers play in access control and the cryptographic processes commonly used? Exploration of integration with access control systems could provide valuable insights into future-proofing against quantum threats.

References:

1. “Usable characters for user names and passwords,” *Ricoh.com*, 2025. https://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001050/0001050898/view/security/int/0010.htm (accessed Jan. 01, 2025).

2. “How to Calculate Password Entropy?,” *Password Generator*. https://generatepasswords.org/how-to-calculate-entropy/

3. Wikipedia Contributors, “Side-channel attack,” *Wikipedia*, Jul. 10, 2019. https://en.wikipedia.org/wiki/Side-channel_attack

4. S. Simonson and T. Woodcock, “The Five-Button Door Lock - Experiment and Discovery in Mathematics,” *Recreational Mathematics Magazine*, vol. 8, no. 14, pp. 105–125, Oct. 2021, doi: https://doi.org/10.2478/rmm-2021-0006.

5. “Math Goes Pop! - Secure Your Phone with Pretty Pictures,” *Mathgoespop.com*, 2018. https://www.mathgoespop.com/2011/03/secure-your-phone-with-pretty-pictures (accessed Jan. 01, 2025).

6. A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge Attacks on Smartphone Touch Screens.” Available: https://www.usenix.org/legacy/events/woot10/tech/full_papers/Aviv.pdf

7. D. Lucian and C. D. Lucian, “Chubb Detector Lock - Antique Box Guide,” Antique Box Guide, Apr. 24, 2015. https://www.antiquebox.org/chubb-detector-lock/ (accessed Jan. 01, 2025).

8. “Schuyler Towne | Rethinking the Origins of the Lock,” *Schuylertowne.com*, 2025. https://schuylertowne.com/research/rethinking-the-origins-of-the-lock (accessed Jan. 01, 2025).

9. Wikipedia Contributors, “Security information and event management,” *Wikipedia*, Nov. 27, 2019. https://en.wikipedia.org/wiki/Security_Information_and_Event_Management

10. Thales, “Technology: One Time Password (OTP),” *www.thalesgroup.com*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp

11. M. or break, “RSA SecurID hardware token reverse engineering,” *Flow.gi*, 2022. https://flow.gi/SecurIDReverseEngineering/ (accessed Jan. 01, 2025).

12. “Understanding Zero Trust. What is it? | SSLTrust,” *www.ssltrust.com*. https://www.ssltrust.com/blog/understanding-zero-trust

13. K. Raina, “What is Zero Trust Security? Principles of the Zero Trust Model | CrowdStrike,” *Crowdstrike.com*, Apr. 17, 2023. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

14. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” csrc.nist.gov, Aug. 11, 2020. https://csrc.nist.gov/pubs/sp/800/207/final

15. “On the discussion of security vulnerabilities,” *Mattblaze.org*, 2025. https://www.mattblaze.org/hobbs.html (accessed Jan. 01, 2025).

16. Wikipedia Contributors, “Kerckhoffs’s principle,” *Wikipedia*, Dec. 17, 2019. https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

17. “Enclave,” *Ominoushum.com*, 2025. https://ominoushum.com/lock/ (accessed Jan. 01, 2025).

18. KnowTheBird, “High Security Locking Mechanism with Zoned Adherence Keyway,” 2023. https://drive.google.com/file/d/1FRtN6xx_wFrPaDLZ-8AsfbUTEzPIkot2/view?usp=sharing

19. Fey, “Evolution of Abloy (Part 3),” Sep. 2005. https://toool.nl/images/8/8a/Abloypart3.pdf

20. G. Pulford, *High-Security Mechanical Locks*. Butterworth-Heinemann, 2007.

21. J. Bramah, A Dissertation on the Construction of Locks. 1785. Available: https://ouverture-fine.com/storage/2020/05/A_Dissertation_on_the_Construction_of_Locks_1785.pdf

22. “USPS.com FAQs,” *Usps.com*, 2022. https://faq.usps.com/s/article/Registered-Mail-The-Basics

23. UPS, “UPS Express Critical Secure.” https://www.ups.com/media/en/UPS-Express-Critical-Secure.pdf (accessed Jan. 01, 2025).

24. “High Security Shipping: Anti-interdiction in 2021 – Purism,” *Purism*, Jan. 03, 2022. https://puri.sm/posts/high-security-shipping-anti-interdiction-in-2021/ (accessed Jan. 01, 2025).

25. P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis.” Available: https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf

26. P. Kocher, J. Jaffe, and B. Jun, “Introduction to Differential Power Analysis and Related Attacks,” 1998. https://www.rambus.com/wp-content/uploads/2015/08/DPATechInfo.pdf (accessed Jan. 01, 2025).

27. “Filter Connectors - Amphenol Canada,” *Amphenolcanada.com*, 2019. https://www.amphenolcanada.com/category/filter-connectors (accessed Jan. 01, 2025).

28. “DPA Countermeasures.” Accessed: Jan. 01, 2025. [Online]. Available: https://www.rambus.com/wp-content/uploads/2018/11/DPA-Countermeasures-Solution-Overview.pdf

29. J. Weyers, M. Burrough, W. Belgers, BandEAtoZ, and N. Tolley, *Locksport*. No Starch Press, 2024.

30. Marc Weber Tobias, *LOCKS, SAFES, AND SECURITY*. Charles C Thomas Publisher, 2000.

31. “What are BS3621 Locks? + How to tell you have British Standard Lock,” *Master Locksmiths Association*. https://www.locksmiths.co.uk/faq/what-are-bs3621-british-standard-locks/

32. KnowTheBird, “Prioritize” *GitHub*, 2022. https://github.com/knowthebird/Prioritize (accessed Jan. 01, 2025).

33. naswek, “How reverse sidebars work.,” *YouTube*, Dec. 12, 2021. https://www.youtube.com/watch?v=JVz-t9FvK3A (accessed Jan. 19, 2025).

34. “Yuema 750 / Forte Enigma,” *LPU Belt Explorer*, 2025. https://share.lpubelts.com/?id=0b604114&name=Yuema_750___Forte_Enigma (accessed Jan. 19, 2025).

35. “Chubb Mark IV Manifoil - Lockwiki,” *Lockwiki.com*, 2023. https://www.lockwiki.com/index.php/Chubb_Mark_IV_Manifoil (accessed Jan. 19, 2025).

36. Artichoke2000, “Disc Detainer Lock Info/Guides,” *Google Docs*, 2019. https://docs.google.com/document/d/13e4pwKJuaZ6vyfnE35NIN2SVGz-vGelEFwFBb9JAZY0/edit?tab=t.0 (accessed Jan. 19, 2025).

37. “Lock Picking 101 Forum • How to Pick Locks, Locksport, Locksmithing, Locks, Lock Picks.,” *Lockpicking101.com*, 2019. https://www.lockpicking101.com/viewtopic.php?f=35&t=65606 (accessed Jan. 19, 2025).

38. HelpfulLockPicker, “What Is MACS and Why Are There Limits On How You Can Cut Your Key?,” *YouTube*, Dec. 30, 2020. https://www.youtube.com/watch?v=KSKIVl0IyQo (accessed Jan. 19, 2025).

39. “Differs - Lockwiki,” *Lockwiki.com*, 2025. https://www.lockwiki.com/index.php/Differs (accessed Jan. 19, 2025).

40. “MY TIME LOCK COLLECTION,” *My-time-machines.net*, 2025. https://www.my-time-machines.net/my_time_lock_collection.htm (accessed Jan. 19, 2025).

41. “Security Ratings - Lockwiki,” *Lockwiki.com*, 2022. https://www.lockwiki.com/index.php/Security_Ratings (accessed Jan. 19, 2025).

42. “Home - SKG-IKOB Certificatie,” *www.skgikob.nl*. https://www.skgikob.nl/

43. “Digby Lock and Tool LLC,” *Digby Lock and Tool LLC*, 2025. https://digbylockandtool.com/ (accessed Jan. 19, 2025).

44. Lock Noob, “The Bravo Custom Made Lock from Digby Lock and Tool,” *YouTube*, Apr. 16, 2024. https://www.youtube.com/watch?v=LQtEuu-U4VQ (accessed Jan. 19, 2025).

45. Panda-Frog, “Exclusive Achievement: Successfully Picking the Serialized Digby Lock and Tool Bravo Lock!,” *YouTube*, Aug. 18, 2023. https://www.youtube.com/watch?v=pLgQ0XMuHWk (accessed Jan. 19, 2025).

46. E. Andrews, “What Was the Gordian Knot?,” *HISTORY*, Feb. 03, 2016. https://www.history.com/news/what-was-the-gordian-knot

47. “Gordian Knot,” *Wikipedia*, Mar. 04, 2020. https://en.wikipedia.org/wiki/Gordian_Knot

48. “Table 19,” *FBI*. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/tables/table-19

49. “Special Report,” 2010. Available: https://bjs.ojp.gov/content/pub/pdf/vdhb.pdf

50. electronicsNmore, “Gallium Vs Aluminum & 14 Different Metals! How Will they React? Find Out!,” *YouTube*. Oct. 21, 2019. Accessed: May 13, 2022. [Online]. Available: https://www.youtube.com/watch?v=UP_NvmRAllw

51. “Compatibility by Material,” *www.calpaclab.com*. https://www.calpaclab.com/chemical-compatibility-by-resin-material/

52. B. DeWall, “Bypassing Doors – Part 3: REX Sensor,” *Cyberadvisors.com*, May 12, 2022. https://blog.cyberadvisors.com/technical-blog/blog/bypassing-doors-part-3-rex-sensor (accessed Jan. 19, 2025).

53. “Red Team Tools REX Blaster Nozzle Head (Gen 3),” *Redteamtools.com*, 2025. https://www.redteamtools.com/rex-blaster-nozzle-head-gen-3 (accessed Jan. 19, 2025).

54. “Easy Entrie Key Blank Milling Machine V9.0+ (230V - Voltage Converter Required for USA),” *MBA USA, Inc.*, 2025. https://mbausa.com/easy-entrie-key-blank-milling-machine-v9-0-230v-voltage-converter-required-for-usa/ (accessed Jan. 19, 2025).

55. “Medeco Programs Quick Reference Guide.” https://content.assaabloyusa.com/doc/AADSS1246745 (accessed Jan. 18, 2025).

56. “Modular Vaults & Safes Solutions for GSA Approved Containers & DEA Approved Dispensary Medical Cannabis & Marijuana, SCIF Facility Security DOD, Government & Business Enterprise Security Solutions.,” *Klsecurity.com*, 2015. https://www.klsecurity.com/index.php/ (accessed Jan. 19, 2025).

57. “Gate Key Switches and Padlocks - Knox Rapid Access System,” *Knoxbox.com*, 2022. https://www.knoxbox.com/Products/Gate-Key-Switches-and-Padlocks (accessed Jan. 19, 2025).

58. M. W. Tobias and T. Bluzmanis, *Open in Thirty Seconds*. 2008.

59. “Trapped Key Interlocking: Enhancing Safety, Compliance, and Cost Savings,” *Linkedin.com*, 2025. https://www.linkedin.com/pulse/trapped-key-interlocking-enhancing-safety/ (accessed Jan. 19, 2025).

60. DeviantOllam, “Can You Identify All 10 of These Door Handle Type? (Categories of Door and Latch Functions),” *YouTube*, Nov. 06, 2023. https://www.youtube.com/watch?v=ItK9y0sPtWg (accessed Jan. 19, 2025).

61. “Keynote - LockPickingLawyer,” *www.youtube.com*. https://www.youtube.com/watch?v=IH0GXWQDk0Q (accessed Mar. 14, 2022).

62. “Dual User Setup - S&G,” *S&G*, Jun. 04, 2020. https://sargentandgreenleaf.com/knowledgebase/knowledgebase-2017-02-24-dual-user-setup/?srsltid=AfmBOopepvzq8sNNoZ256FvCASaqs-smpJ1gCskqVZXRPhssZYsfP9Cd (accessed Jan. 19, 2025).

63. “Lever Padlocks - Antique Padlocks,” *Antique-padlocks.com*, 2025. https://antique-padlocks.com/lever_iron_blank.htm (accessed Jan. 19, 2025).

64. *UFC 4-420-10, Internal Locking Device for Magazine Doors*. DOD.

65. “OPERATING INSTRUCTIONS X-10 TM Type 1F HIGH SECURITY ELECTRONIC LOCK.” Accessed: Jan. 19, 2025. [Online]. Available: https://exwc.navfac.navy.mil/Portals/88/Documents/EXWC/DoD_Locks/PDFs/X-10-operating-instructions.pdf

66. M. Levenson, “How a Company That Makes Gun Safes Angered Gun Owners,” *The New York Times*, Sep. 08, 2023. Available: https://www.nytimes.com/2023/09/08/business/liberty-safe-codes.html

67. Shopify API, “Policy for FBI and Law Enforcement Information Demands,” *Liberty Safe*, Oct. 04, 2023. https://www.libertysafe.com/pages/policy-for-fbi-law-enforcement-information-demands (accessed Jan. 19, 2025).

68. Michael Maynard, “[135] Tutorial - Master rings, moguls, pin states, and maths,” *YouTube*, Apr. 22, 2018. https://www.youtube.com/watch?v=cccU3Xf5HPE (accessed Jan. 19, 2025).

69. Lock Pickers United, “Master Keyed SFIC Picking Analysis,” *YouTube*, Oct. 18, 2020. https://www.youtube.com/watch?v=_WZP454BEIU (accessed Jan. 19, 2025).

70. M. Blaze, “Rights amplification in master-keyed mechanical locks,” *IEEE Security & Privacy*, vol. 1, no. 2, pp. 24–32, Mar. 2003, doi: https://doi.org/10.1109/msecp.2003.1193208.

71. LockPickingLawyer, “[1360] Carbine Dual Entry Padlock Picked,” *YouTube*, Sep. 15, 2021. https://www.youtube.com/watch?v=LejwsIc3yVY (accessed Jan. 19, 2025).

72. LockMan28, “[34] ‘LIKA’ Dual Cylinder, Double Sided Dimple Lock (PICKED!),” *YouTube*, Mar. 28, 2015. https://www.youtube.com/watch?v=1t050YYHbuM (accessed Jan. 19, 2025).

73. “LOCK KEY - Owner restricted replacement key,” *Bowley Lock Company Inc*, 2025. https://www.bowleylockcompany.com/store/p7/LOCK_KEY_-_Owner_restricted_replacement_key.html (accessed Jan. 19, 2025).

74. J. Wilkes, “How a SAFE is Designed (Part 1: Ingenious Engineering Against Attack) - Mechanical Engineering,” *Mechanical Engineering*, Oct. 07, 2017. https://mechanical-engineering.com/how-a-safe-is-designed/ (accessed Jan. 19, 2025).

75. “Security Now! #974 -05-14-24.” Accessed: Mar. 06, 2025. [Online]. Available: https://www.grc.com/sn/sn-974-notes.pdf

76. Enzoic, “8 Scary Statistics about the Password Reuse Problem,” *Enzoic*, Apr. 30, 2020. https://www.enzoic.com/blog/8-stats-on-password-reuse/

77. HackerOne, “Why You Need Responsible Disclosure and How to Get Started,” *www.hackerone.com*, 2023. https://www.hackerone.com/knowledge-center/why-you-need-responsible-disclosure-and-how-get-started

78. Marc Weber Tobias, *Tobias on Locks and Insecurity Engineering*. John Wiley & Sons, 2024.

79. “Submit Vulnerability Report,” *@AllegionCorp*, 2025. https://www.allegion.com/corp/en/footer/security/vulnerability-report.html (accessed Mar. 06, 2025).

80. “Manual 5200.01, Volume 3,” 2013. https://exwc.navfac.navy.mil/Portals/88/Documents/EXWC/DoD_Locks/PDFs/DODM-5200-01-vol3.pdf

81. “Manual 5100.76, Change 2,” 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510076m.pdf

82. A. C. Hobbs and C. Tomlinson, Rudimentary Treatise on the Construction of Locks. London: Weale, 1853.

Frequently Asked Questions:

1. Do I need a high security lock?
    a. If you work with the Department of Defense, classified material, weapons, schedule I/II narcotics, controlled substances, biological pathogens, bank safes, vaults, or ATMs, there are very likely legal requirements for you to have locks with higher security certifications. Many other industries will have legal requirements for locks from a safety perspective (commercial buildings, educational buildings, apartments, hotels, daycare), but they are not typically what we would classify “high security”. Insurance companies may require locks with security certifications for higher levels of coverage.
2. Do I want a high security lock?
    a. Yes, they are pretty cool :-)
3. What lock do you recommend?
    a. This depends on the use case and budget. I would not recommend an Abloy PL 362 for a middle school gym locker, and I would not recommend using locks made of plastic to secure unattended firearms. There are a lot of important nuances to access control, like building and fire codes for your local area, which is why I recommend talking to a professional with access control experience familiar with your area. This can also help determine what the most common attacks are in your area, so you know what you need to defend against.
4. What is a “Pick Proof” lock?
    a. There is no single definition for “Pick Proof”. But there are many floating around. Each describes various aspects of lock security that may be desirable to different users. There is no one right answer for everyone.
        - One that can only be opened with the key that was made for it.
        - One that cannot be opened with lock picks.
        - One where the time to manipulate is greater than ## minutes, hours, days, years, depending on the system.
        - One where the time to manipulate the lock is long enough it can be reasonably expected the attacker would choose another method.
        - One that provides no feedback.
        - One where the fastest method to pick open is to try all possible combinations (manipulation is no faster or efficient than brute force)
        - One that will permanently lock if an attempt to open it is made with the wrong key.
        - One where any attempt to open the lock is detected.
5. Are “Pick Proof” locks possible?

a. This depends on what is meant by “Pick Proof”. Because access control systems use conditional security, there is always some chance they can be accessed by an unauthorized user. The probability of gaining access in a given time is a more quantifiable and verifiable characteristic. There are of course other terms that can measurably or definitively describe a lock's resistance to manipulation.

Common Misconceptions:

1. "All locks can be opened with enough time and the right tools."
    a. While this statement is largely true, it oversimplifies security and can lead to complacency. Not all locks and safes passively yield to attack.
        i. Some locks and safes are designed with countermeasures that destroy or mark contents or activate security protocols when tampered with or after multiple failed access attempts. Tamper detection mechanisms, such as relocking devices, can significantly increase resistance to forced entry.
        ii. Assuming that all locks will eventually fail ignores the reality that well-designed security systems buy critical time, deter attackers, and introduce serious risks for unauthorized access attempts.
2. You get what you pay for with security, more expensive means more secure:
    a. While very cheap locks will often not offer many security features, it is not true that if a lock is expensive, it is secure. There are many locks sold for many hundreds of dollars that can be opened in seconds and are less secure than locks that are a small fraction of the price. Manufacturer’s advertising is rarely a candid self-assessment, and referring to third party evaluations is always preferred.
3. Sharing vulnerabilities publicly reduces security and exposes consumers to danger.
    a. Irresponsibly sharing vulnerabilities can reduce security and expose consumers to danger by giving attackers an upper hand and “element of surprise”. If shared responsibly, after first contacting manufacturers and security professionals, and giving industry reasonable time to prepare and deploy mitigations and patches, the information provides consumers and manufacturers a more realistic perspective of their security and the opportunity to improve it.
        i. *“Rogues knew a good deal about lock-picking long before locksmiths discussed it… If a lock is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are… certain to apply the knowledge practically… the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.”* A.C. Hobbs, Rudimentary Treatise on the Construction of Locks, 1853. [82]
4. Electronic locks are immune to picking or manipulation.

    a. As discussed in the paper, electronic locks can provide feedback like mechanical locks. They typically interface simply with a mechanical system, and that interface can be a primary target for manipulation.

5. Encryption is irrelevant in digital lock design because, ultimately, doors are opened by mechanical components.
    a. In addition to making certain attacks to access a single system harder, encryption adds another layer of security against privilege escalation attacks on other systems after one system has been compromised.
6. “Do not duplicate” on a key means it cannot be copied.
    a. This text on a key is not legally binding. It is more like a polite request. Unique key shapes, restricted key blanks, patent control, and one-time passwords (OTP) provide better protection against copying.
7. Lockpicking takes years to master.
    a. To become proficient in picking a variety of high security locking mechanisms will likely take years, however, there are many locks people can learn to pick open in minutes. At conferences with lockpicking villages, TOOOL volunteers will often teach dozens of people to pick their very first locks in under 20 minutes.
8. Tolerances build up from cumulative manufacturing errors and are what makes picking locks possible.
    a. This is a simplification specific to a certain style of manipulation for a certain lock. It is helpful when teaching lock picking to someone new to it, but wrong in a broader context. All locks will have tolerances due to manufacturing errors. This may or may not provide useful feedback to an attacker. Even with perfect manufacturing tolerances, feedback would exist due to the laws of thermodynamics, and this too may or may not provide useful feedback to an attacker. It is the lock design that determines if feedback is useful and determines what forms of picking may be possible.
9. Locksmith [So-and-So] said the lock is unpickable and that the videos online showing its defeat are fake.
    a. This is a common defense mechanism used to protect reputations or prevent public concern. Locksmiths are not always security experts and may lack practice and skill in lock bypass and manipulation techniques, but just because one person has never opened a lock, does not mean others have not. Many reputable lockpicking experts, including those in the locksport community, document their work with transparent methods that can be reproduced.
10. I saw a video on YouTube of the lock being opened in 30 seconds, it must be a joke.
    a. People generally upload videos showcasing their best attempts. A single video does not provide key context, such as the lockpicker’s experience level, prior knowledge of the keying, the number of practice attempts, the repeatability of the attack on the

same lock, or whether it can be replicated across other locks of the same model. Due to these variables, any single video of a lock being opened—whether quickly or slowly—should be considered just one data point within a broader security assessment.

Maximum Adjacent Cut Specification (MACS) Effects on Possible Keys

To introduce some of the general concepts, we ignored a common constraint specific to pin tumbler permutations called the Maximum Adjacent Cut Specification (MACS). This specification states the maximum amount of variance between two keying values and prevents bitting values from being used that would either get stuck in the lock or cause significant wear [38]. It varies between different locks and manufacturers but will further reduce the number of possible keys significantly.

Because of the recursive and conditional nature of MACS, it is not trivial to write a closed form for the number of possible keys. Instead, we have opted to generate these in software, and the source code for these calculations is provided in the appendix. Some may look at these numbers and think they are unrealistic. To that we suggest taking in the context that many experienced lockpickers will be able to open each of these locks listed in under a minute. That is without perfect feedback, and without optimized equations to prevent testing the same key twice. If we also consider the tolerances of these locks, we may see the theoretical limits on the number of possible keys to test is lower for some of these brands.

While the exact values are not of much value, this is also interesting because we can see cases where a key might perform less well against a brute force attack but then be slightly more resilient against manipulation attacks.

Brand	K	N	MACS	Theoretic, No MACS	Theoretic, W/ MACS	W/ MACS, Perfect Feedback, Order of Key Testing Matters	W/ MACS, Perfect Feedback, Order of Key Testing Does Not Matter
Sargent	10	6	7	1,000,000	753,754	170	47
Weiser	10	5	5	100,000	44,692	112	34
Kwikset	7	6	4	117,649	65,449	107	29
Schlage	10	7	7	10,000,000	7,131,596	223	54
Yale	10	7	5	10,000,000	3,027,314	193	44
Arrow	10	6	7	1,000,000	753,754	170	47
Weslock	10	5	6	100,000	62,948	118	37

Maximum Number of Possible Keys to Test

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

from itertools import product
from math import ceil


def high_low_sequence(start, end):
    if start > end:
        return []
    numbers = list(range(start, end + 1))
    result = []
    low, high = 0, len(numbers) - 1
    while low <= high:
        result.append(numbers[high])
        high -= 1
        if low <= high:
            result.append(numbers[low])
            low += 1
    return result


def all_permutations(num_positions, num_depths):
    return product(range(num_depths), repeat=num_positions)


def macs_valid(combination, macs):
    valid = True
    for i in range(1, len(combination)):
        if abs(combination[i] - combination[i - 1]) > macs:
            valid = False
            break
    return valid


def calculate_macs_compliant_keys(num_positions, num_depths, macs):
    total_permutations = all_permutations(num_positions, num_depths)
    valid_permutation = []
    for permutation in total_permutations:
        if macs_valid(permutation, macs):
            valid_permutation.append(permutation)
    return len(valid_permutation)
```

```
def total_keys_with_macs_feedback_order_does_not_matter(
    num_positions, num_depths, macs
):

    valid_combinations = []
    rev_sequence = high_low_sequence(0, num_depths - 1)[::-1]
    combination = [rev_sequence[0]] * num_positions

    for i in high_low_sequence(0, num_depths - 1):
        combination[0] = i
        if macs_valid(combination, macs):
            valid_combinations.append(combination[:])

    for i in range(1, num_positions)[::-1]:
        for j in high_low_sequence(0, num_depths - 1)[::-1]:
            combination[i] = j
            if macs_valid(combination, macs):
                if combination not in valid_combinations:
                    valid_combinations.append(combination[:])
    return len(valid_combinations)


def total_keys_with_macs_feedback_order_does_matter(num_positions, num_depths, macs):

    total_keys = 0
    new_keys = total_keys_with_macs_feedback_order_does_not_matter(
        num_positions, num_depths, macs
    )
    total_keys = total_keys + new_keys

    for i in range(1, num_positions)[::-1]:
        new_keys = (
            total_keys_with_macs_feedback_order_does_not_matter(i, num_depths, macs) - 1
        )
        total_keys = total_keys + new_keys

    return total_keys


if __name__ == "__main__":
    num_positions = int(input("Enter the number of positions on the key (n): "))
    num_depths = int(input("Enter the number of unique depths available (k): "))
```

```
    macs = int(input("Enter the MACS value: "))

    possible_keys = all_permutations(num_positions, num_depths)
    possible_keys = [keys for keys in possible_keys]
    print(
        "Total number of keys possible without any feedback and without MACS requirements: ",
        len(possible_keys),
    )

    possible_keys = calculate_macs_compliant_keys(num_positions, num_depths, macs)
    print(
        "Total number of keys possible without any feedback with MACS requirements: ",
        possible_keys,
    )

    possible_keys = total_keys_with_macs_feedback_order_does_matter(
        num_positions, num_depths, macs
    )
    print(
        "Total number of keys possible with perfect feedback, and with MACS requirements, and the
order keys are tested matters: ",
        possible_keys,
    )

    possible_keys = total_keys_with_macs_feedback_order_does_not_matter(
        num_positions, num_depths, macs
    )
    print(
        "Total number of keys possible with perfect feedback, and with MACS requirements, and the
order keys are tested does not matter: ",
        possible_keys,
    )
```

Manipulation Resistance Estimate Guide:

Manipulation Resistance Estimate Guide

Score	Bypass Possible	Lock Out and Time Delay Features	Feedback	Keying Bits of Entropy	Keying Resettable	Staging and Interlocks	Obstructions	Detection (Logs, Seals, and Alarms)
9 Strong	No	Permanent After Single Failed Attempt	No Useful Feedback	> 128	Yes and required periodically, No OEM Master Backup, Reset Does Not Require (Tools, Training, Admin)	Decoupled interfaces and Group must Reset to baseline	No Keyway – no port available to access locking mechanism	Yes, log valid and invalid attempts remote, no reset
8	Yes - Config. Dependent, Tools Required, internal damage	Permanent After Multiple Failed Attempts	Group Feedback with False Gates	> 112	Yes and required initially, No OEM Master Backup, Reset Does Not Require (Tools, Training, Admin)	Decoupled interfaces and individual must Reset to baseline	No Keyway – but port available to access locking mechanism	Yes, remote indication, can not be reset
7	Yes - Config. Dependent, Tools Required, no internal damage	Permanent After Attack Detected	Group Feedback	> 96	Yes, No OEM Master Backup, Reset Does Not Require (Tools, Training, Admin)	Decoupled interfaces and Some Reset Required for Individual	Keyway inaccessible when keying checked	Yes, remote indication, can be reset remotely
6	Yes - Config. Dependent, No Tools Required	Temporary After Single Failed Attempt	Indirect Individual Feedback with False Gates	> 80	Yes w/ Admin, No OEM Master Backup, Reset Does Not Require (Tools, Training)	Decoupled interfaces	Non-linear keyway, (requires flexible moving key)	Yes, remote indication, can be reset locally
5	Yes – Tools Required – internal damage	Temporary After Multiple Failed Attempts	Direct Individual Feedback with False Gates	> 64	Yes, No OEM Master Backup, Reset Requires Tools/Training	Group must Reset to baseline	Passive Pins	Yes, log valid and invalid attempts local, no reset
4	Yes – Tools Required – No internal damage, keys remain secret	Temporary After Attack Detected	Indirect Individual Feedback, Ordering does matter	> 48	Yes, No OEM Master Backup, Reset Requires 3rd Party	Some Reset Required for Group	Curtain and warding	Yes, local indication, can not be reset
3	Yes – Tools Required – No internal damage, keys revealed	Temporary Time Based	Direct Individual Feedback, Ordering does matter	> 32	No, OEM MFR Does Not Retain Record	Individual must Reset to baseline	Curtain	Yes, but reset with correct key
2	Yes – No Tools Required, keys remain secret	Temporary User Engaged	Indirect Individual Feedback, ordering does not matter	> 16	Yes, But OEM MFR retains Master Backup	Some Reset Required for Individual	Warding or Paracentric Keyway	Yes, but auto resets after time delay
1 Weak	Yes – No Tools Required, keys revealed	None	Direct Individual Feedback, Ordering does not matter	> 1	No – OEM MFR Retains Record	None	None	None