Optimal Threshold Padlock Systems

Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Léo Robert

Optimal Threshold Padlock Systems

Jannik Dreier* Jean-Guillaume Dumas† Pascal Lafourcade‡
Léo Robert‡

April 23, 2020

Abstract

In 1968, Liu described the problem of securing the documents in a shared secret research project. In his example, at least six out of eleven participating scientists need to be present to open the lock securing the secret documents. Shamir proposed a mathematical solution to this physical problem in 1979, by designing the first efficient k-out-of-n secret sharing scheme based on a smart usage of Lagrange's interpolation. Shamir also claimed that the minimal solution using physical padlocks is *clearly impractical* and exponential in the number of participants. In this paper we propose an optimal physical solution to the problem of Liu that uses physical padlocks, but the number of locks is at most equal to the number of participants. This device is optimal for k-out-of-n threshold padlock systems as soon as $k > \sqrt{2n}$. We also propose an optimal scheme implementing a 2-out-of-n threshold padlock system requiring only about $2\log_2(n)$ padlocks. Then we derive some lower bounds required to implement threshold systems in general. Finally, we discuss more complex access schemes together with other realizations with strictly less than n padlocks.

1 Introduction

In 1979, in his paper on secret sharing [25], Shamir presented the following threshold problem introduced by Liu in [16]: *Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?* Shamir answered to this *physical* problem using mathematics as follows: *It is not hard to show that the minimal solution uses 462 locks and 252 keys per scientist. These numbers are clearly impractical, and they become exponentially worse when the number of scientists increases.* This is why he proposed to use polynomial and Lagrange's interpolation to

*Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
†Université Grenoble Alpes, IMAG-LJK, CNRS UMR 5224, Grenoble, France
‡Université Clermont Auvergne, LIMOS, CNRS UMR 6158, Aubière, France

solve Liu's question. His clever idea is to hide the secret in the constant term of a polynomial of degree $k-1$. Then he distributes one point of the chosen polynomial to each of the n participants. As soon as k participants share their points, they can recover the secret using Lagrange's interpolation. As discussed in [1, 14], there are algorithms in $O(n \log^2 n)$ for the Lagrange's interpolation that are better than the straightforward quadratic algorithm. A few years later, verifiable secret sharing was introduced by Chor et al. in [7] and improved in [10]. The idea is to offer the possibility to verify if the points are valid.

We show that one can solve Liu's problem using far less locks than Shamir claimed. Shamir's claim stems from the restriction that there should be a lock for each combination of 6 scientists, $462 = \binom{11}{6}$, and that every scientist needs the keys for every combination of scientists that includes him. This is $252 = \binom{10}{5}$ keys. Shamir's minimality result thus assumes that the only physical arrangements of locks that allow threshold systems are those where the opening of any lock opens the cabinet.

Contributions: We design a physical k-out-of-n threshold lock system and build a prototype of the device. Our system only requires one lock and one key per participant, which is practical comparing to the solution proposed by Shamir in [25].

Moreover, we establish lower bounds on the number of padlocks necessary for a particular abstract threshold system. Specifically, we show that for a 2-out-of-n configuration, $2\lceil \log_2(n) \rceil$ locks are sufficient provided that keys can be duplicated. We further show that there is an optimal solution for this type of configuration, with $\mathcal{O}(\log(n))$ padlocks, and we also show that this optimum can be realized, using our physical system as one building block.

Differently, for k-out-of-n configurations with $k \geq 3$, it is more complicated to go beyond n padlocks. We first prove that this is impossible for $k > \sqrt{2n}$ and thus that our device is optimal in these cases. We are then nonetheless able to build systems for $k = 3$ with only $\mathcal{O}(\sqrt{n})$ padlocks and each participant owns 3 keys. These realizations use more complex access policies, like for instance ensuring that Alice and Bob can open the lock with any other third participant, but not together. For this we develop a tentative of *padlock algebra* and give associated algorithms.

For instance, we were also able to answer Liu's question: the minimal number of padlocks for a 6-out-of-11 configuration is 11. Our system with 11 padlocks and only 1 key per participant, is thus optimal in this case.

For these theoretical results, we combine threshold cryptography and secret sharing with the theory of block designs, packings and Sperner families.

Outline: In Section 2, we review existing threshold mechanisms that use physical locks or visual cryptography. We show that each kind of existing solutions does not perfectly answer Liu's problem. In Section 3, we describe our novel physical k-out-of-n threshold lock system. In Section 4, we derive generic bounds on the number of locks required to realize a given threshold configuration. We finally discuss more complex access schemes in Section 5, together with lower bounds and smaller realizations with strictly less than n padlocks in Section 6.

2 Related Work

Threshold cryptography in general received a lot of attention recently, since on March 1, 2019 the Computer Security Division (CSD) at the National Institute of Standards and Technology (NIST)[1] published the final version of NISTIR 8214, "*Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography*[2]. Note that NIST explicitly also mentions physical threshold solutions (page 10, line 55): "*While we focus on secure implementations of cryptographic primitives, the actual threshold techniques may also include non-cryptographic techniques.*" We present existing physical solutions for threshold cryptography, while a survey of cryptographic threshold schemes by Yvo Desmedt can be found in [8]. We distinguish two classes of solutions: the first one uses physical keys and locks; the second one uses visual cryptography, as introduced by M. Naor and A. Shamir in 1994 [22].

2.1 Using Locks

The case of 1-out-of-1 lock is just the usage of one simple physical lock. We found many systems for 1-out-of-n locks, both home made and commercial products. There exists also commercial solutions for n-out-of-n locks, which are used by for example by electricians to secure an electrical circuit as explained below.

2.1.1 1-out-of-n locks

In Figure 1, left, a 1-out-of-2 locks is done simply with two physical locks. This approach can be generalized to 1-out-of-n as in Figure 1, right, and is called a

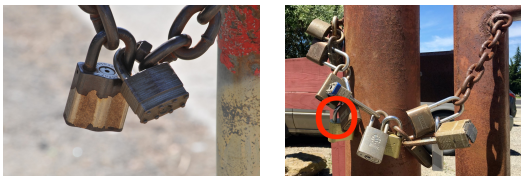

Figure 1: Physical 1-out-of-n locks, forming a daisy chain.

daisy chain. We notice that the bottom left yellow lock was badly placed, and it is useless. In this case the owner of this lock cannot open the door. We call this the *daisy chain attack*. For example in Figure 1, if the owner of the bottom lock opens it and then locks it upper in the chain, then he excludes all the owners of these locks, as they cannot open the door any more[3].

In Figure 2, we can see two different mechanisms that perform 1-out-of-6 locks to open the gate of a field. On the left side, there are six locks that block

[1] CSD aims at promoting the security of implementations cryptographic primitives.

[2] https://csrc.nist.gov/Projects/threshold-cryptography

[3] Note that a deliberate attack adding an additional chain and lock to the gate, or even welding locks together, is always possible, and out of scope here. We aim to protect against an attack that could be "excused" with a wrong use of the locking system.

Figure 2: Two ad-hoc physical 1-out-of-6 locks.

the trigger. As soon as one lock is opened a latch is removed and then the door can be opened. It is the natural extension of the solution of Figure 1 that avoids the daisy chain attacks.

On the right side of Figure 2, we have a different solution also implementing a 1-out-of-6 lock, and which is also resistant to the daisy chain attack. In this

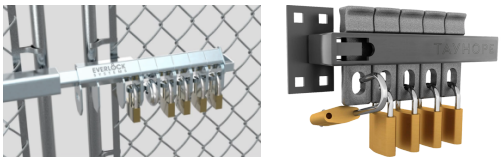

Figure 3: Physical 1-out-of-5 locks by Tayhope multi-locking system on right side and Everlock System on the left side.

system, as soon as one lock is removed, it is possible to turn the circle and then to pass the stick in the corresponding hole in order to open the door.

There are also commercial products for 1-out-of-n locks. The left side of Figure 3 shows a commercial product designed by Everlock Systems: the model SLX2[4]. This solution uses a different idea, but is close to the mechanism proposed on the left side of Figure 2. Everlock Systems has multiple patents on their designs [17, 18, 19, 20]. The right side of Figure 3 shows a commercial product sold by Tayhope Multi-Locking Systems[5]. This mechanism allows the owner of a lock to remove the metallic stick which enables the opening of the door, by pushing all the locks on one side.

2.1.2 n-out-of-n locks

Finally, there are physical n-out-of-n mechanisms using locks that are used for example for operations on high-voltage circuits and transformers. Two examples of 6-out-of-6 locks are given in Figure 4. The idea is that nobody should be able to turn on the electricity while someone is still working on the high-voltage transformer. To achieve this, each technician places a lock on the main switch before entering the danger zone. This ensures that all technicians have to leave

[4] A video of Everlock System SLX2 is available https://vimeo.com/180052349

[5] A video of Tayhope Multi-Locking Systems http://sancy.univ-bpclermont.fr/~lafourcade/VIDEOS/secu/tayhope_voiceover.mp4

Figure 4: Physical 6-out-of-6 locks, by Seton (models SLECO and MANM8).

the danger zone before electricity can be restored. The example can easily be extended to a n-out-of-n system.

2.2 Using Visual Cryptography

In 1994, M. Naor and A. Shamir proposed the *visual cryptography* [22, 23] for black and white images. This was improved in [4] for gray images and in [12] for color images. The idea is to split a secret into two images printed on transparent

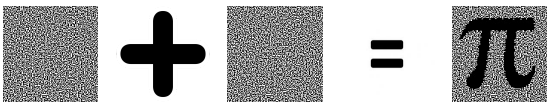

Figure 5: Example of visual cryptography, superposing the images let the symbol π appear.

paper in a way such that their superposition makes the secret appear. An example is given in Figure 5.

For color images, security cannot be perfectly achieved for more than 3 colors [15]. In [27], the authors proposed a generalization of the approach to k-out-of-n images. This can be used as a first physical answer to Liu's problem. This solution is not really practical since it needs a computer to compute the different images. Moreover in [11], the authors show that it is possible to cheat in visual cryptography by introducing fake shares that change the result. This clearly shows that this solution is not verifiable, which requires the ability to check that shares are valid.

3 Physical k out n Threshold Lock

We design a k-out-of-n physical threshold lock that uses n padlocks and works as follows. Each lock secures one block, with a latch, attached to a sliding bar, which is limited in its sliding movement by the blocks. If sufficiently many blocks are removed, the sliding bar can be moved far enough to open the barrier. We built a wooden prototype that can be configured for different cases, see Figure 6 for a 2-out-of-3 configuration. Appendix A contains further example configurations.

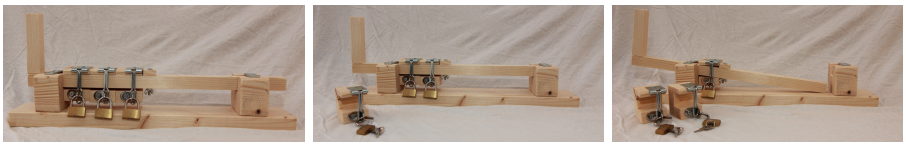

Figure 6: Physical 2-out-of-3 lock. **Left:** all three blocks attached, lock closed. **Middle:** one block removed, the bar can be moved to the left, but not sufficiently far to open. **Right:** two locks are removed, the barrier is open.

Our technique can also be used to implement *weights* by using blocks of different sizes. Figure 7 shows an example where either one "master" key (opening the padlock on a larger block) can be used to open the lock, or any two of the other keys (opening the padlocks on the smaller blocks). The same idea can also be used to implement a policy where, e.g., either Alice and one other participant, or any three other participants are required to open the lock. It suffices to give Alice the keys for the larger block, and use a configuration that requires the removal of three small blocks to open.

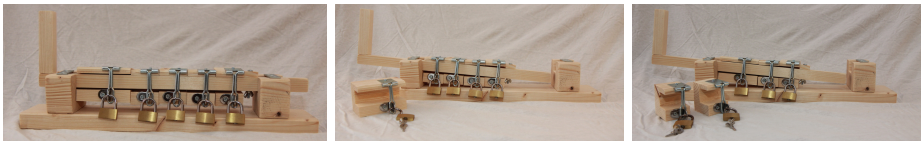

Figure 7: Physical lock with weighted keys. **Left:** all blocks are attached and locked. **Middle:** the "master" key was used to open the larger block, unlocking the barrier. **Right:** two "normal" keys opening normal blocks also allow to open the barrier.

Our system is *ad-hoc* since once it is set up, each participant can install their own lock, which avoids having to trust the dealer as in existing cryptographic solutions. Note that to avoid problems during the setup phase, we assume that all participants install their locks at the same time, right after the lock has been set up.

Our solution is also *reusable* as it can be locked again, unlike for example a solution using cryptographic secret sharing to share a code for a combination lock, where the code would be revealed once and for all: such a lock thus cannot be effectively locked again without changing the code. Note that a system with a combination lock would also require a special procedure or a trusted third party to setup the combination initially. Moreover, our system also protects users against the *daisy chain attack* as only one padlock can be fitted to the latch of any block.

By construction our solution is *verifiable* since everyone can check if there is at least one lock that can be opened with the secret key that he has received.

Comparing to the mathematical solution proposed in [10] consisting in giving extra information to each participant to convince him that he received a valid point of the polynomial, our solution does not require any extra material. There are at least three direct applications of our physical threshold system:

1. Our system can be used to construct a physical verifiable secret sharing protocol. As it can also easily be extended to deal with weights, we also have a physical equivalent to the cryptographic protocol given in [2, 9].
2. Threshold cryptography has been applied to voting, e.g., in [24]. Our system can be used to secure physical pen and paper voting, by ensuring that the ballot box can only be opened if k-out-of-n trustees agree.
3. As a user never has to reveal his physical key, our mechanism can also be used to design an k-out-of-n authentication mechanism.

4 Generic Bounds on the Number of Padlocks

We now establish bounds on the number of padlocks required to realize a certain threshold. The proofs are given in Appendix B. We assume that padlocks are more expensive than keys, i.e., we will try to implement threshold systems with less padlocks, even if this means duplicating some of the keys. We define a padlock system to be any arrangement of padlocks protecting something. For the sake of simplicity, in the following, we consider this to be the possibility to open a door.

Definition 1. *A* padlock *is a device requiring a single* key *to be opened. A* padlock-system *is an arrangement of padlocks that prevents a* door *to be opened. Keys can be duplicated.*

Definition 2. *A* k-threshold padlock system *is an arrangement of padlocks and a distribution of keys that allows any group of* k *or more participants to open the door and prevents any group of strictly less than* k *participants to open it.*

Remark 3. *While directly applicable to physical padlock systems, this definition also applies to some cryptosystems. For instance consider any symmetric or asymmetric cryptosystem with a shared (duplicated) decryption key. Closing a padlock could just be ciphering with an encryption key; setting a padlock-system could just be multiple encryption (even if electronic threshold cryptosystem are more complicated) and opening the door is deciphering. For this example, the only difference with physical system is that the order of encryption must be taken into account for decryption.*

Now, most of the lower *bounds described in this section only suppose the existence of a threshold system satisfying the above definitions. Therefore those lower bounds also apply to electronic threshold cryptosystem satisfying Definitions 1 and 2.*

Definition 4. *Let* n *be the number of players and* $k \leq n$ *be a threshold of players required to open the "door". Then* $\ell_{k,n}$ *is the minimal number of padlocks, in any arrangement, allowing a* k*-out-of-*n *threshold opening of the door. Also, we*

define the rank of an arrangement of padlocks and keys as the maximal number of keys owned by any player.

For instance, we have that:

- $\ell_{1,n} = 1$: one padlock with everybody having a copy of the same key is sufficient.
- $\ell_{k,n} \leq n$: by our system described in Section 3, see Figure 6.

4.1 Sperner Families

Using the fact that all subsets of size k of the n participants can open the door, and no subset of $k-1$ or less can do it, we have the following results. First, it is easy to see that with only $k-1$ or less different locks, one cannot ensure a threshold of at least k.

Lemma 5 (Appendix B)**.** $\forall k \geq 2, \ell_{k,n} \geq k$.

Second, if the set of keys of a participant is included in another participant's set of keys, intuitively the first participant is "useless" to achieve the threshold.

Lemma 6 (Appendix B)**.** *Let $k \geq 2$, and set up an arrangement of padlocks and a distribution of keys with a k-out-of-n threshold opening. No participant can own a set of keys that is a subset of another participant's set of keys.*

This shows for instance that each participant must have at least one key. Further, this means that the sets of keys must form a family of inclusion-free subsets. This is called a *Sperner family* or a *clutter* [26]. The padlocks can then be seen as the vertices of an hypergraph, where each participant is represented by an hyperedge, the set of its owned keys. The *rank* is then the maximal cardinality of an hyperedge. Then Sperner's Theorem combined with Lemma 6, also gives the following three lower bounds:

Corollary 7 (Appendix B)**.** $\forall n, t$ *and* $k \geq 2$*, if* $\ell_{k,n} = t$ *then* $\binom{t}{\lfloor t/2 \rfloor} \geq n$.

Corollary 8 (Appendix B)**.** $\forall n \geq 1$ *and* $\forall t \geq 2$ *even, if* $k \geq 3$ *and* $\ell_{k,n} = t$ *then* $\binom{t}{\lfloor t/2 \rfloor} > n$.

Lemma 9 (Appendix B)**.** $\forall n \geq 3, \ell_{2,n} \geq 3$.

We have thus now for instance the following results:

- $\ell_{n,n} = n$: use Lemma 5 for the lower bound and our design for the upper bound.
- $\ell_{2,3} = 3$: use Lemma 9 for the lower bound and our design for the upper bound.

4.2 Using $\mathcal{O}(\log(n))$ Padlocks for a Threshold of 2 with n Participants

Now we propose, in Algorithm 1, an arrangement for a 2-out-of-n participants threshold system, using no more than n padlocks, and strictly less as soon as $n \geq 5$. Indeed if the threshold is only 2, then it is possible to reduce the number of padlocks using our design. We first deal with small cases:

Theorem 10 (Appendix B). *$\forall n \leq 5, \forall k \geq 2, \ell_{k,n} = n$, except $\ell_{2,5} = 4$. We also have $\ell_{2,6} = 4$ and $\forall n = 7..10, \ell_{2,n} = 5$.*

The case $\ell_{2,5} = 4$ uses a 3-out-of-4 lock, where each participant has a different set of two out of the four keys. Hence any two participants together have at least three different keys, which allows to open the lock, but no participant can open the lock alone as he lacks one key. This is illustrated in Figure 9 in Appendix A.

Algorithm 1 Two-out-of-n threshold system with shared keys

Require: $n \geq 2$, and $1 \leq i \leq t \leq n$ such that $\binom{t}{i} \geq n$.
Ensure: A 2-out-of-n threshold padlock system with t padlocks.

if $t < n$ **then**
    Set up an $(i+1)$-out-of-t design of Section 3;
    Create a total of $i \cdot n$ keys by copying the original t keys, such that there are n distinct subsets of i keys;
    Give each participant a distinct i-tuple of keys.
else ▷ If $t = n$, set $i = 1$ and use directly our device of Section 3
    Set up a 2-out-of-n design of Section 3;
    Give each participant one of the n keys.
end if

We give an asymptotic estimate for larger cases: it is possible to implement a 2-out-of-n threshold padlock system with only $2\lceil \log_2(n) \rceil$ padlocks and $n\lceil \log_2(n) \rceil$ keys:

Proposition 11 (Appendix B). *Algorithm 1 is correct and for $n \geq 2$, $\ell_{2,n} \leq 2\lceil \log_2(n) \rceil$.*

For instance, the first case where triples are better than couples in Algorithm 1 is for $n = 16$. As $\binom{6}{2} = 15$ and $\binom{7}{2} = 21$, with pairs the Algorithm would use 7 padlocks, where 6 are enough: setup a 4-out-of-6 device and give distinct triples of copies of the 6 keys to each of the 16 participants. This is possible as $\binom{6}{3} = 20 \geq 16$. Then any pair of participants have at least $3 + 1 = 4$ different keys and they can open our device.

Overall, we have that the minimal number of padlocks for a 2-out-of-n threshold system is $\mathcal{O}(\log(n))$ with $\mathcal{O}(n \log(n))$ keys:

Corollary 12 (Appendix B). *For $n \geq 2$, $\ell_{2,n} = \min \left\{ t \text{ such that } \binom{t}{\lfloor t/2 \rfloor} \geq n \right\}$.*

The lower bound is given in Corollary 7, and it is realizable by Algorithm 1.

4.3 For a Larger Threshold, a Larger Rank is Required

Finally, we show that for thresholds larger than 3 things are more complicated. The main idea is that for larger thresholds, if there are less than n padlocks, as soon as all the subsets of size k can open the door, there will very often be a subset of size $k-1$ also able to open the door, contradicting the assumption.

Theorem 13 (Appendix B)**.** *For $k \in \{3, 4, 5, 6\}$, $\ell_{k,6} = 6$.*

Lemma 14 (Appendix B)**.** *For $k \geq 3$ in a k-out-of-n threshold system, if the rank of the arrangement is 2 or less, then the number of padlocks is at least n.*

To go beyond n padlocks, for threshold larger than 3, we need more gadgets. In particular, in the rest of the paper, we show how to combine devices while using the same padlocks.

5 Towards a Padlock Algebra

A generalization of threshold schemes is to be able to implement any access scheme described by a logic formula. This is possible by implementing AND and OR gates, as shown in Proposition 15 and Algorithms 2 and 3. A first idea is to use chains so that opening a padlock actually frees a chain that can free several latches. Then a second idea is that 1-out-of-n systems are just like a disjunction while n-out-of-n systems are just like a conjunction.

Proposition 15. *Any disjunctive or conjunctive normal form with t clauses, m distinct literals and no negation is realizable with m padlocks*

Proof. First for disjunctive clauses: they require one 1-out-of-t threshold system and m chains, as said in Algorithm 2. The "door" can be opened only by a satisfiable interpretation where TRUE means opening the padlock and FALSE means letting it closed.

Algorithm 2 Physical DNF with one padlock for each literal

1: Set up a 1-out-of-t threshold system, with one latch for each clause;
2: For each literal present in the formula: pass a chain through the hole of each latch corresponding to a disjunction containing that literal; close that chain with one padlock.

Similarly one can create arrangements for conjunctive normal forms, also with as many padlocks as there are literals as shown in Algorithm 3.

Algorithm 3 Physical CNF with one padlock for each literal

1: Set up a t-out-of-t threshold system;
2: Create one tree for each disjunctive clause. Each tree is a composition of 2-out-of-2 devices, so as to have the number of literals holes in the tree. Attache each tree to one of the t latches of the t-out-of-t system.
3: For each literal present in the formula: pass a chain through any hole of each tree corresponding to a clause containing that literal; close that chain with one padlock.

□

Appendix C gives also further existing commercial building blocks that can ease the implementation of Algorithms 2 and 3, especially for trees. This appendix also shows that these physical realizations provide solutions where secret sharing alone is insufficient.

6 Square Root Bounds for Threshold Systems

We now have tools to deal with larger thresholds. First we give a necessary condition for systems using less than n padlocks. This enables us to show that our device is optimal when k is larger than $\sqrt{2n}$. For instance, we fully answer Liu's question about the smallest number of locks needed to implement a 6-out-of-11 threshold system. Then, the necessary condition, together with block design theory and our padlock algebra of Section 5, enables us to build padlock systems with strictly less than n padlocks: systems with only $\sqrt{n}$ padlocks for 3-out-of-n thresholds.

6.1 A Necessary Condition and the Answer to Liu's Problem

We first begin with a necessary condition.

Proposition 16 (Appendix D)**.** *$\forall n$ and $\forall k \geq 3$, if a k-out-of-n threshold system uses strictly less than n padlocks, then apart from participants owning the single key of a given padlock, the other participants must satisfy:*

1. *Their sets of keys have minimal mutual distance larger than 2;*
2. *Each of them owns at least k distinct keys.*

We can now fully answer Liu's question with Theorem 17, $\ell_{6,11} = 11$. The theorem also shows that our system is optimal for all $k \geq \frac{\sqrt{8n+1}-1}{2}$.

Theorem 17 (Appendix D)**.** $\ell_{k,n} \geq \min\{n, k(k+1)/2\}$.

6.2 Packings, Johnson Bound and a 3-threshold Realization for up to 12 Participants with only 9 Padlocks

Proposition 16 shows that a minimal k-threshold system with less than n padlocks must contain a $(2,1)-$packing, as defined thereafter:

Definition 18 (See e.g. [6])**.** *Let n, k, and p be integers with $n > k > p \geq 2$. Let λ be a positive integer. A $(p,\lambda)-$*packing *of order n, and blocksize k is a set V of n elements, and a collection B of k-element subsets (blocks) of V, so that every p-subset of V appears in at most λ blocks.*

Finally, Jonhnson's bound [13], states that a maximal packing has a number of blocks upper bounded by:

$$\left\lfloor \frac{t}{k} \left\lfloor \frac{t-1}{k-1} \right\rfloor \right\rfloor . \tag{1}$$

To be able to give a k-subset of keys to each player, where any pair of subsets do not share a pair of keys then the latter must be larger than n. This suggests that systems with $t = \mathcal{O}(k\sqrt{n})$ padlocks might be possible.

Unfortunately, Proposition 16 is probably not sufficient: it might possible to fulfill its condition while still having some set of players of size strictly lower than k having the same set of keys as some set of players of size k. We prove that for $k = 3$ we can always use Steiner triplet systems to build 3-threshold systems. As a consequence, it is possible to build a 3-threshold padlock system with only $\mathcal{O}(\sqrt{n})$ padlocks.

Proposition 19 (Appendix D)**.** *Any Steiner triangle system gives rise to a* 3*-threshold system.*

In Appendix E, we give the smallest example realizing Proposition 19: a 3-out-of-12 system, with only 9 padlocks, 36 keys and 82 latches, and an example using normal forms to reduce the number of latches for a 3-out-of-12 system with only 11 padlocks, 36 keys and 33 latches. Finally, by setting up a minimal Steiner system for any number of players we have the following upper bound of $\mathcal{O}(\sqrt{n})$ for the number of padlocks:

Theorem 20 (Appendix D)**.** $\ell_{3,n} \leq 6 \left\lceil \frac{\sqrt{24n+1}-5}{12} \right\rceil + 3$.

7 Conclusion

We designed a physical k-out-of-n threshold lock that can be used for various applications, including physical access control, voting or secret sharing. Our system only uses n padlocks, showing that Shamir's answer to Liu's problem was not optimal. For $k = 2$, we were even able to identify a more efficient solution using our system, which only needs $2\lceil \log_2(n) \rceil$ padlocks, but requires duplicating keys. Further, we were able to build an optimal solution with $\mathcal{O}(\log(n))$ padlocks. Finally, we devised algorithms that can implement more complex access policies beyond simple thresholds, expressed as Boolean formulas.

There are however some open questions left, for example explore the links with digital systems, or finding minimal solutions in terms of padlocks for k between 3 and $\sqrt{2n}$, or for more complex access policies. For the former case, when $k \geq 3$, Johnson's bound suggests that it might be possible to build systems with only $\mathcal{O}(k\sqrt{n})$ padlocks and we were able to prove this for $k = 3$. In the latter case, it is also unclear whether there are general solutions using less locks than the number of literals.

Finally, if we not only count the number of padlocks, but more generally the number of keys or of latches, then clearly a lower bound on the number of devices

is n: each player must at least have something. Otherwise groups of k players with an empty player would have the same abilities of a group of $k-1$ players. With this model of complexity, our k-out-of-n designs are asymptotically optimal as they require just n padlocks, n latches and n keys.

References

[1] A. V. Aho and J. E. Hopcroft. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Longman Publishing Co., Inc., USA, 1st edition, 1974.

[2] A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. In *Proceedings of the Second International Conference on Theory of Cryptography*, TCC05, page 600619, Berlin, Heidelberg, 2005. Springer-Verlag.

[3] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology — CRYPTO' 88*, pages 27–35, New York, NY, 1990.

[4] C. Blundo, A. D. Santis, and M. Naor. Visual cryptography for grey level images. *Inf. Process. Lett.*, 75(6):255–259, 2000.

[5] R. C. Bose. On the construction of balanced incomplete block designs. *Annals of Eugenics*, 9(4):353–399, 1939.

[6] Y. M. Chee, C. J. Colbourn, A. C. Ling, and R. M. Wilson. Covering and packing for pairs. *Journal of Combinatorial Theory, Series A*, 120(7):1440 – 1449, 2013.

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, SFCS 85, page 383395, USA, 1985.

[8] Y. Desmedt. Threshold cryptography. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 1288–1293. Springer US, 2011.

[9] O. Farras and C. Padro. Ideal hierarchical secret sharing schemes. *IEEE Transactions on Information Theory*, 58(5):3273–3286, May 2012.

[10] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, SFCS 87, page 427438, USA, 1987. IEEE Computer Society.

[11] G. Horng, T. Chen, and D.-S. Tsai. Cheating in visual cryptography. *Des. Codes Cryptography*, 38(2):219236, Feb. 2006.

[12] Y.-C. Hou. Visual cryptography for color images. *Pattern Recognition*, 36(7):1619 – 1629, 2003.

[13] S. M. Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962.

[14] D. E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., USA, 1997.

[15] B. W. Leung, F. Y. Ng, and D. S. Wong. On the security of a visual cryptography scheme for color images. *Pattern Recognition*, 42(5):929 – 940, 2009.

[16] C. L. Liu. *Introduction to combinatorial mathematics*. McGraw-Hill New York, 1968.

[17] R. McNeil. Multiple padlock latch. US Patent Number US6857299B2, 2003.

[18] R. McNeil. Multiple padlock lock system. US Patent Number US7503194B2, 2008.

[19] R. McNeil. Multiple padlock locking device. US Patent Number US7503194B2, 2014.

[20] R. McNeil. Multiple padlock locking system. US Patent Number US9702169B2, 2015.

[21] E. C. Milner. A combinatorial theorem on systems of sets. *Journal of the London Mathematical Society*, s1-43(1):204–206, 1968.

[22] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques*, pages 1–12, 1994.

[23] M. Naor and A. Shamir. Visual cryptography II: improving the contrast via the cover base. In *Security Protocols, International Workshop, Cambridge, United Kingdom, April 10-12, 1996, Proceedings*, pages 197–202, 1996.

[24] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *In CRYPTO*, pages 148–164. Springer-Verlag, 1999.

[25] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[26] E. Sperner. Ein Satz über die Untermengen einer endlichen Menge. *Mathematische Zeitschrift*, 27:544–548, 1928.

[27] E. R. Verheul and H. C. A. Van Tilborg. Constructions and properties of k-out-of-n visual secret sharing schemes. *Des. Codes Cryptography*, 11(2):179196, May 1997.

A Appendix: further configurations of our prototype

Figure 8, left, shows our prototype in a 2-out-of-4 configuration. The prototype can be configured for k-out-of-n systems for any $k \in \{1, 2, 3\}$ and $n \in \{3, 4, 5, 6\}$. By moving the wooden block attached to the moving bar (red circle in Figure 8, right) one can fix the number of blocks that can be attached, i.e., n. By moving the block on the right (blue circle in Figure 8, right) one can fix the number of blocks that need to be removed before the bar can be opened, i.e., the threshold k: on the rightmost position, removing one block is sufficient to open the bar. When moving this block to the left one can increase the number of blocks that need to be removed before the bar opens. For convenience, in our prototype everything can be easily adjusted using screws, but obviously, in a real implementation, they need to be permanently fixed to ensure security.

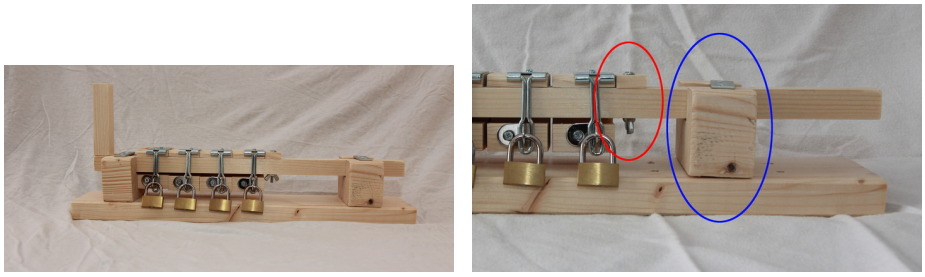

Figure 8: **Left:** Physical 2-out-of-4 threshold padlock system; **Right:** configuring our prototype: the block in the red circle fixes the number n (here: 4), the block in the blue circle fixes the threshold k (here: 3). One can also see the holes that allow the block to be fixed in other positions.

Figure 9 shows our prototype in a 3-out-of-4 configuration. As explained in Section 4.2, using Algorithm 1, this configuration can also be used to implement a 2-out-of-5 with only four padlocks by copying keys and distributing them in such a way that each participant has a distinct subset of keys (as stated in Theorem 10). In this example, any two participants together will have at least three different keys, which suffices to open the 3-out-of-4 device.

B Appendix: proofs of Section 4

We here gives proofs for the results of Section 4.

Lemma 5 (Appendix B)**.** $\forall k \geq 2, \ell_{k,n} \geq k$.

Proof. Suppose for $\ell_{k,n}$ we have an existing threshold system where a minimum of k people is required to open the door, and moreover any subset of k people

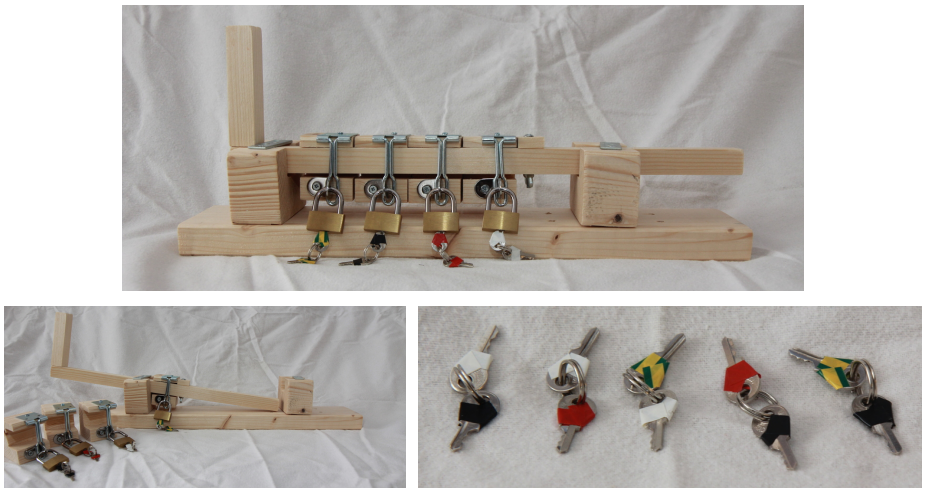

Figure 9: Physical 3-out-of-4 threshold padlock system. **Top:** all locks closed. **Left bottom:** device opened using 3 out of the 4 locks. **Right bottom:** Example key distribution to achieve a 2-out-of-5 threshold system using only 4 padlocks and the 3-out-of-4 device above (see Section 4.2, Algorithm 1 and Theorem 10).

can open it. Suppose $t = \ell_{k,n} \leq k-1$ and consider one group of k people able to open the door. For this, whatever the arrangement, they had to open some of the t padlocks, thus with at most t keys. This is less keys than the number of people, so there must exist a subgroup of at most t people owning these t keys. This subgroup of size at most t is thus able to open the door by themselves. But $t \leq k-1 < k$, is thus below the threshold, a contradiction. □ □

Lemma 6 (Appendix B)**.** *Let $k \geq 2$, and set up an arrangement of padlocks and a distribution of keys with a k-out-of-n threshold opening. No participant can own a set of keys that is a subset of another participant's set of keys.*

Proof. Let A have a set of keys included in that of B. As $k \geq 2$, A and B can be in a size k subset of participants that can open the door. But then the keys of A are useless since B has all of them. Therefore there would be a size $k-1$ subset of participants able to open the door, a contradiction. □ □

Corollary 7 (Appendix B)**.** *$\forall n, t$ and $k \geq 2$, if $\ell_{k,n} = t$ then $\binom{t}{\lfloor t/2 \rfloor} \geq n$.*

Proof. By Sperner's Theorem, the size of any Sperner family with t elements is upper bounded by $\binom{t}{\lfloor t/2 \rfloor}$. Distributing keys for t padlocks to n participants while satisfying Lemma 6 thus requires $\binom{t}{\lfloor t/2 \rfloor} \geq n$. □ □

Corollary 8 (Appendix B)**.** *$\forall n \geq 1$ and $\forall t \geq 2$ even, if $k \geq 3$ and $\ell_{k,n} = t$ then $\binom{t}{\lfloor t/2 \rfloor} > n$.*

Proof. By Corollary 7, the only other possibility is $n = \binom{t}{\lfloor t/2 \rfloor} = \binom{t}{t/2}$. But then the unique available Sperner family is that of all subsets of equal size $t/2$. In this family there exist pairs of subsets with an empty intersection. The union of these two subsets is thus of exactly t keys and must be able to open the door. Therefore the threshold cannot be larger than 2. □ □

Lemma 9 (Appendix B)**.** $\forall n \geq 3, \ell_{2,n} \geq 3$.

Proof. Suppose $\ell_{2,n} = 2$. Then, if a single person has both keys, she can open both padlocks. Hence, whatever the arrangement of padlocks, she can open the door alone and $k < 2$, a contradiction. Therefore nobody can have more than one key. As $k = 2$, then two persons are sufficient to open the door. They cannot have the same key by Lemma 6. But with only 2 distinct keys and $n \geq 3$ people, at least two persons must have the same key, a contradiction again. Overall, 2 padlocks are thus not enough. □ □

Theorem 10 (Appendix B)**.** $\forall n \leq 5, \forall k \geq 2, \ell_{k,n} = n$*, except* $\ell_{2,5} = 4$*. We also have* $\ell_{2,6} = 4$ *and* $\forall n = 7..10, \ell_{2,n} = 5$.

Proof. For any $n \leq 3$ and $2 \leq k \leq n$ the results where already proven in Lemma 5 and 9. There remains $n = 4$ and $n = 5$, our design providing the upper bound. The proof is done by contradiction.

Let $t = \ell_{k,n}$ and suppose $t \leq n-1$. Let s be the number of participants having a single key. These participants must have different single keys by Lemma 6. The remaining $n - s$ participants must own at least 2 keys, but cannot own any of the first s keys, by Lemma 6. Each set of keys of these remaining $n - s$ participants cannot be the full set of the remaining $t - s$ keys, again by Lemma 6. Therefore, at least, the number $ds_{s,t}$ of distinct subsets of size at least 2 and at most $t - s - 1$ must be larger than $n - s$ (the requirement is that the size of the clutter, must be larger than $n - s$, but in this clutter all the subsets must at least be distinct). This is:

$$ds_{s,t} = \sum_{i=2}^{t-s-1} \binom{t-s}{i} \geq n - s \tag{2}$$

But, if $t \leq n - 1$ and $n \geq 4$, then:

$$ds_{s,t} \leq \sum_{i=2}^{n-s-2} \binom{n-s-1}{i} = 2^{n-s-1} - 1 - (n-s-1) - (n-s-1) \tag{3}$$

Therefore, Equation (2) cannot be satisfied whenever Equation (3) is $< n - s$, that is:

$$2^{(n-s)-1} < 3(n-s) - 1 \tag{4}$$

But Equation (4) is true for $n - s \in \{1, 2, 3, 4\}$. Yet $n - s > 1$, otherwise $n - 1 \geq t \geq s$ implies at most $t = s = n - 1$, but then there remains no available key for the n-th participant. Hence, we have $n - s \in \{2, 3, 4\}$.

For $n = 4$, if $s \in \{2, 1, 0\}$ then Equation (4) is satisfied thus we can dismiss those cases. Finally, there exists no value for s meaning that our hypothesis $t \leq n - 1$ is false.

For $n = 5$, if $s \in \{3, 2, 1\}$ then Equation (4) is also satisfied so we can dismiss those cases. There remains the case $s = 0$ for $t = 4$ (the case $t = 3$ is excluded by the fact that $\binom{3}{2} = 3 < 5$). The 5 participants can thus only have 2 or 3 keys each (if one of them has the 4 keys he can open the door alone). If one of the 5 participants owns 3 keys K_1, K_2, K_3 then the other four must all own the fourth key K_4 (otherwise one of them will own only a subset of the first 3 keys, contradicting Lemma 6). But then, excluding K_4, these four remaining participants must have distinct non-included subsets of size 1 or 2 of the 3 keys K_1, K_2, K_3, which is impossible. Therefore the rank of the arrangement is 2, that is, all 5 participants can only have 2 keys each. There are $\binom{4}{2} = 6$ possible pairs. W.l.o.g. suppose that only the pair K_3, K_4 is not among the participants pairs.

Then two participants owns (K_1, K_3) for one and (K_2, K_4) for the other, so the two of them can open all the padlocks. This means that $k \leq 2$. For $k > 2$, we have a contradiction since no value s can be taken leading to refute the hypothesis $t \leq n - 1$. Thus for $n = 5$ and $k \geq 3$ we have $\ell_{k,n} = n$.

The remaining case, $k = 2$ is thus actually 2-out-of-5 threshold with at least 4 padlocks where every player owns exactly 2 keys.

This is satisfiable as follows: use a 3-out-of-4 device with our design with 4 padlocks. Then provide the 5 users with distinct pairs of keys. Not a single user can open 3 padlocks. But with distinct pairs of keys all pairs of participants own at least 3 different keys.

Finally, Algorithm 1 gives a solution as soon as t is such that $\binom{t}{2} \geq n$, while Corollary 7 prevents any solution with $\binom{t}{\lfloor t/2 \rfloor} < n$. But with $t = 4$ and $t = 5$, $\binom{t}{2} = \binom{t}{\lfloor t/2 \rfloor}$. So the upper bound of Algorithm 1 is also a lower bound. Now $\binom{4}{2} = 6$ and $\binom{5}{2} = 10$ give the maximal respective number of participants. □ □

Proposition 11 (Appendix B)**.** *Algorithm 1 is correct and for $n \geq 2$, $\ell_{2,n} \leq 2\lceil \log_2(n) \rceil$.*

Proof. Consider an $(i+1)$-out-of-t threshold system with t padlocks for $\binom{t}{i} \geq n$. Distribute i keys for each participant, such that all the hyperedges are distinct. This is possible as $\binom{t}{i} \geq n$. No single participant can open the device, but any two participants have different hyperedges of size i and thus have at least $i + 1$ distinct keys. This is enough to open the door and Algorithm 1 is correct. Finally, $\binom{t}{i} \geq (t/i)^i$, so we can for instance set $i = \lceil \log_2(n) \rceil$, so that each participant gets that many keys, and set up $t = 2\lceil \log_2(n) \rceil$ padlocks, as $2^{\lceil \log_2(n) \rceil} \geq n$. □ □

Corollary 12 (Appendix B)**.** *For $n \geq 2$, $\ell_{2,n} = \min \left\{ t \text{ such that } \binom{t}{\lfloor t/2 \rfloor} \geq n \right\}$.*

Proof. The lower bound is given by Corollary 7. For the upper bound consider as in Proposition 11 an $(\lfloor t/2 \rfloor + 1)$-out-of-$t$ threshold system with t padlocks

and distribute $\lfloor t/2 \rfloor$ keys to each participant, such that all the hyperedges are distinct. □ □

Theorem 13 (Appendix B)**.** *For $k \in \{3,4,5,6\}$, $\ell_{k,6} = 6$.*

Proof. Again the upper bound is given by our new design.

Then, let $\ell_{k,6} = t$. By Corollary 7, $t \geq 4$ (indeed $\binom{3}{1} = 3 < 6$).

If $t = 4$, then the unique Sperner family of maximal size is given by the 6 distinct pairs of keys. But then there exists a couple of pairs with all keys distinct, that can therefore open the 4 padlocks. Therefore if $t = 4$, the threshold cannot be greater than 2.

Now, if $t = 5$ padlocks, by Equation 2, there can be only $s = 0$ or $s = 1$ participants with a single key. If $s = 1$ then the remaining five participants must have a Sperner family of 4 keys with 5 subsets. This is possible only with pairs, so that the configuration is w.l.o.g. $K_0; (K_1, K_2); (K_1, K_3); (K_1, K_4); (K_2, K_3); (K_2, K_4)$. But then $(K_1, K_2) \cup (K_1, K_3) \cup (K_1, K_4) = (K_1, K_3) \cup (K_2, K_4)$ so a subset of 3 participants has exactly the same keys as a subset of 2 participants. Therefore if $t = 5$ and $s = 1$, the threshold cannot be greater than 2.

There remains the case $s = 0$, so all participants have more than 2 keys. No participant can have 4 keys or more (otherwise there are at most $5 < 6$ subsets of keys). So all participants have 2 or 3 keys.

Not all participants can have 3 keys: Milner's generalization of Sperner's Theorem states that the cardinality of any Sperner family where every pair of subsets has intersection larger 2 has cardinality lower than $\binom{5}{\lfloor (5+2+1)/2 \rfloor} = 5 < 6$ [21, Theorem 1]. So at least one pair of subsets out of the 6 subsets has an intersection of size 1. Therefore these two participants have $3 + 3 - 1 = 5$ keys, that is *all* the keys, and the threshold cannot be greater than 2.

Suppose there is at least one participant with 3 keys K_1, K_2, K_3.

- All other participants have 2 keys, there remains only 7 possible pairs to give to 5 participants. The type of the pairs that are not given is (up to renumbering) of type $(K_3K_5; K_4K_5)$ or $(K_3K_4; K_3K_5)$ or $(K_1K_4; K_3K_5)$. In all these cases there remain $(K_1K_4; K_2K_4; K_2K_5)$. But this triple contains the same keys as the couple $(K_1K_4; K_2K_5)$. Therefore the threshold cannot be greater than 2.

- If there are other participants with 3 keys, none of their intersections can be of size only 1, with the same argument as above.

  - Then if there are two participants with three keys, $K_1K_2K_3; K_1K_2K_4$, or three participants with three keys $K_1K_2K_3; K_1K_2K_4; K_1K_3K_4$, then not both K_3K_5 and K_4K_5 can be avoided as pairs of the remaining participants. But then for instance the couple of participants $(K_1K_2K_3; K_4K_5)$ holds all the keys and the threshold cannot be greater than 2.
  - If there are 4 participants with 3 keys $K_1K_2K_3; K_1K_2K_4; K_1K_3K_4; K_2K_3K_4$, then w.l.o.g. a fourth participant has K_5K_1 but then the couple $(K_5K_1; K_2K_3K_4)$ again has all the keys.

– If there are five participant with 3 keys, then at least one couple must have an intersection of size 1 and this couple has all the keys.

So finally the only remaining possibility is that all the six participants have only distinct pairs of keys. This is a total of 12 keys so at least one key appears three or more times. Therefore w.l.o.g. there exists a triple of participants holding only four keys $K_1K_2; K_1K_3; K_1K_4$. Then the other participants cannot own a pair of keys among K_2K_3; K_2K_4 nor K_3K_4 otherwise there would exist a couple of participants with the same subset as a triple of participants. W.l.o.g. the remaining participants thus have the pairs $K_5K_1; K_5K_2; K_5K_3$. But then the triple $K_1K_2; K_5K_1; K_5K_2$ has the same subset of keys as, e.g. the couple $K_1K_2; K_5K_1$.

Finally there are no threshold systems for k-out-of-6 with strictly less than 6 padlocks than can have a threshold greater than 2. □ □

Lemma 14 (Appendix B)**.** *For $k \geq 3$ in a k-out-of-n threshold system, if the rank of the arrangement is 2 or less, then the number of padlocks is at least n.*

Proof. If the rank is 1, then all participants have a distinct single key and thus the number of padlocks is at least n.

Now if the rank is 2, let t be the number of padlocks in a k-out-of-n arrangement.

If there exists a participant with a single key, that key cannot be given to any other participant by Lemma 6. Now between the other $n - s$ participants, on the one hand, if $k \leq (n - s)$, they cannot share the keys for less than $\ell_{k,n-s}$ other padlocks. On the other hand, if $k > (n - s)$, complete the group of $n - s$ with $k - n + s$ singleton, they cannot use less than $\ell_{k,k} = k$ padlocks, that is $n - s$ new padlocks for the $n - s$ group. As $n - s = \ell_{n-s,n-s}$, we have shown that for any number s of participants with a single key, the following holds:

$$t \geq s + \ell_{\min\{k,n-s\},n-s} \tag{5}$$

Now consider only the subset of participants all having pairs of keys.

Suppose that there exist 2 participants with one key in common. Say $(K_1K_2; K_1K_3)$. Then neither the key K_2, nor the key K_3 can be given to another participant. Indeed, suppose w.l.o.g. that a third participant owns K_2K_i, then a couple of participants has the same keys as a triple of participants: $\{K_1; K_3\} \cup \{K_2; K_i\} = \{K_1; K_2\} \cup \{K_1; K_3\} \cup \{K_2; K_i\}$. This is impossible for a threshold system with $k \geq 3$, as any subset of size k of participants with this triple of participants will have the same keys as a subset with $k - 1$ participants. This shows that for the c pairs of participants sharing a common key then:

$$t \geq 2c + \ell_{\min\{k,n-2c\},n-2c} \tag{6}$$

Finally all the remaining h participants have pairs of keys with an empty intersection, this means that:

$$t \geq 2h + \ell_{\min\{k,n-h\},n-h} \tag{7}$$

Overall, as Theorem 10 and Theorem 13 state that $\ell_{k,n} = n$ for $k \geq 3$ and $n \leq 6$, then Equations (5), (6) and (7) show that the number of padlocks for a larger number of participants can never be lower than n either. □ □

C Appendix: further building blocks for logic formulae

In Section 5, we show that any access scheme described by a logic formula without negation can be implemented using simple physical devices. In this section, We show some other constructions that can simplify the use of Algorithms 2 and 3 for normal forms.

For instance, to implement Algorithm 3 we need a tree of disjunctive clauses. Then Figure 10, left, shows how to create one tree for each disjunctive clause as used in Algorithm 3: assemble U-shaped metal rods. It is also possible to create a daisy chain of 1-out-of-2 devices like the one in Figure 10, right.

Figure 10: Left, a tree-like disjunctive clauses system by GateKeeper GM P6006 to combine 2, 3 or 4 locks; right, a physical 1-out-of-2 disjunction Model Cb2 by Sharelox.

Now we give examples of usage of all our devices and constrction. For this we offer physical solutions for two examples, proven unrealisable using secret sharing. Indeed, [3] shows that the two following cases cannot be solved if users must use the same shares:

1. $(A \wedge B) \vee (C \wedge D)$
2. $(A \wedge B) \vee (B \wedge C) \vee (C \wedge D)$

However, with a physical system, we can easily implement such access schemes as we have tools to implement conjunctions and disjunctions:

- Conjunctions can be implemented with n-out-of-n systems as in Figure 4;
- Disjunctions can be implemented with 1-out-of-n systems as in Figure 3 or in Section 3.

For instance, we first consider the first impossible formula: $(A \wedge B) \vee (C \wedge D)$. We can actually implement Algorithm 2 on this formula, and provide a physical

solution: use a daisy chain of two 2-out-of-2 classical equivalent system, as in Figure 4, one for each conjunction.

For the second formula, $(A \wedge B) \vee (B \wedge C) \vee (C \wedge D)$, a naive implementation would require six padlocks, but it is possible to use only four, as shown in Algorithm 4.

Algorithm 4 Physical realization with only 4 padlocks of [3, Theorem 3]

1: Setup a 1-out-of-3 threshold system (thus with 3 latches);
2: Put a padlock A on the first latch and a padlock D on the third latch;
3: Pass a chain in the holes of the first two latches and close that chain with a padlock B;
4: Pass a chain in the holes of the last two latches and close that chain with a padlock C.

Remark 21. *Finally, note that, with our novel design, Proposition 15 is not optimal. Consider for instance the DNF with a single participant able to open the door or any two among five others:* $A \vee (B \wedge C) \vee (B \wedge D) \vee (B \wedge E) \vee (B \wedge F) \vee (C \wedge D) \vee (C \wedge E) \vee (C \wedge F) \vee (D \wedge E) \vee (D \wedge F) \vee (E \wedge F)$. *Proposition 15 would require* 6 *padlocks and a* 1*-out-of-*11 *design. However, we can use Theorem 10 and our design for a* 3*-out-of-*4 *lock with only* 4 *padlocks as described in Algorithm 5 thereafter.*

Algorithm 5 Physical example with 4 padlocks for 6 literals

1: Set up a 3-out-of-4 design with 4 padlocks;
2: Give pairs of distinct keys to each participant B, C, D, E, F;
3: Give any three distinct keys to A.

D Appendix: proofs of Section 6

Proposition 16 (Appendix D)**.** *$\forall n$ and $\forall k \geq 3$, if a k-out-of-n threshold system uses strictly less than n padlocks, then apart from participants owning the single key of a given padlock, the other participants must satisfy:*

1. *Their sets of keys have minimal mutual distance larger than* 2*;*
2. *Each of them owns at least k distinct keys.*

Proof. We follow the line of proof of Lemma 14. If some users own a single key then this key cannot be reused. More generally, if some user has only a single key not in the set of keys of another, then that key cannot be reused. So we can restrict the analysis to groups of people having sets of keys with minimal distance larger than 2.

Within such a group, suppose that one participant P^* owns a number d of distinct keys strictly lower than the threshold k. Then at least one of his

keys cannot be reused. Otherwise there exists a group of at most d participants owning the same keys as these d participants plus the initial one P^*. As $d < k$, complete these $d+1$ participants with $k-d-1$ others. Those k participants can open the door, as well as the $k-1$ participants obtained when removing P^* from the group. This would contradict the fact that we have a k-threshold system. We have proven: to build a threshold system with strictly less than n padlocks, apart from participants owning the single key of a given padlock, the other participants must satisfy that both their sets of keys have minimal mutual distance larger than 2 and each of them owns at least k distinct keys. □ □

Theorem 17 (Appendix D)**.** $\ell_{k,n} \geq \min\{n, k(k+1)/2\}$.

Proof. For $k = 2$, Lemma 9 gives the result. Now, for $k \geq 3$, let i be the number of players not the single owner of a key and t be the number of padlocks in a k-out-of-n threshold. If $i = 0$, then n players own the single key of a padlock and $t \geq n$. If $i = 1$, then that player has k new distinct keys by Proposition 19 and $t = n - 1 + k \geq n$. If $i = 2$ then one of them has k new distinct keys and the other has at least $k-1$ new ones (otherwise they share a pair of keys). Thus $t \geq n - 2 + k + k - 1$. More generally, if $i \leq k$, then $t \geq n - i + \sum_{j=k-i+1}^{k} j \geq n$. Finally, if $i > k$ then there are at least $\sum_{j=1}^{k} j = k(k+1)/2$ distinct keys. □ □

Proposition 19 (Appendix D)**.** *Any Steiner triangle system gives rise to a* 3*-threshold system.*

Proof. By construction, a Steiner triangle (or triplet) system satisfies the necessary condition of Proposition 16. Second, in order to use it as a 3-threshold system, we want to differentiate triples of triplets from pairs of triplets. Every triplets that have more than 7 distinct values cannot be equated by pairs. By the condition on pairs being uniquely found in a single triplet, triple of triplets have at least 6 distinct values overall. So the only remaining case is to prove that the 6 distinct values of triples of triplets with only 6 distinct values in any construction cannot be found in pairs of triplets of the system.

To have only 6 distinct values any two of the triple of triangles must share one value, and the third one must share a value with each of the two others. W.l.o.g., this is triangles $(a, b, c); (a, d, e); (b, d, f)$, with distinct values a, b, c, d, e, f. Now suppose that these 6 values are contained in a pair of triangles. Then, among a, b, c, at least two of them must be in one of the pair. But by the unicity of triangles containing a given pair this means that (a, b, c) *is* one of the pair. The other pair must now be (d, e, f). But the triangle (a, d, e) is in the system so the pair (d, e) is shared by two different blocks. This is a contradiction and no pair of triangles can share the 6 distinct values of a triple. □ □

Theorem 20 (Appendix D)**.** $\ell_{3,n} \leq 6 \left\lceil \dfrac{\sqrt{24n+1} - 5}{12} \right\rceil + 3$.

Proof. Any construction of a Steiner triangle block design thus works. For instance, Bose construction [5] provides such a design for any $t = 6\nu + 3$.

Proposition 19 proves that these constructions can be used as 3-threshold systems: use a 7-out-of-t design and a large DNF with all the possible groups of 6 distinct values never attained by pairs of participants. Further, Bose construction attain Bound (1) for $t = 6\nu+3$ and $k = 3$, that is $t/3(t-1)/2 = (2\nu+1)(3\nu+1)$. Thus for n players with $n \leq (2\nu+1)(3\nu+1)$ one can set up a Bose construction with $t = 6\nu+3$ and discard the blocks between $n+1$ and $t(t-1)/6$. In other words, for a given n, use $\nu = \left\lceil \frac{\sqrt{24n+1}-5}{12} \right\rceil$ and only $t = 6\nu+3$ padlocks. □ □

E 3-threshold realizations with less than n padlocks

We propose a solution for a 3-out-of-12 system using only 9 padlocks based on the results of Section 6. Indeed, consider the first terms[6] of Equation (1) for $k = 3$ and $t = 0, 1, 2, \ldots$:

$$0, 0, 0, 1, 1, 3, 4, 7, 8, 12, 13, 18, 20, 26, 28, \ldots$$

The smallest t such that Equation (1) is strictly larger than t is for $t = 9$ with a bound of 12 subsets. Hence, packing with 9 padlocks is realizable, for instance with the triplets of keys given in Table 1.

Table 1: A maximal $(2,1)-$ packing of order 9 and blocksize 3. It has 12 blocks.

1	4	7	1	2	3	1	3	2	3	2	1
2	5	8	4	5	6	5	4	6	5	4	6
3	6	9	7	8	9	8	8	7	7	9	8

By inspection, there are 72 triples of triplets (so 3 participants owning each 3 keys) with only 6 distinct keys. The other ones have at least 7 distinct keys (if a triple have a total of less than 5 distinct keys it would mean that at least two of them share a pair). But it turns out that none of the 72 sets of six keys obtained with three triplets can be obtained with only a pair of triplets[7]. The latter ensures that no subset of 2 participants can unlock the door. Further, all these 72 sets of 6 keys are distinct.

Therefore, it is possible to set up a 3-out-of-12 system using only 9 padlocks. The idea is that either a group owns 7 distinct keys or it owns one of the 72 sets of 6 keys not attainable by a pair of participants to open the door. Overall, that solution uses 9 padlocks, 9 chains, 36 keys, a 7-out-of-9 and a 1-out-of-73 design (that is $9 + 73 = 82$ latches). The following process gives a possible solution for such system:

1. Set up 9 padlocks and make 4 copies of each key;

[6] OEIS Foundation Inc. (2020), The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A182079

[7] For instance the triple $(1,2,3);(1,4,7);(2,6,7)$ contains only the six distinct keys $1, 2, 3, 4, 6, 7$, but no pair of triples contain the same set of keys

2. Give 3 keys to each of 12 participants following the packing of Table 1;

3. Set up a 1-out-of-73 design;

4. Set up a 7-out-of-9 design and attach it to one the latches of the $1-7$ design;

5. Use Algorithm 2 to complete the 72 other latches: pass a chain through the hole of each latch corresponding to a disjunction containing that key; close that chain with the associated padlock.

Next, we give a small example where there exists a shortcut to use less latches than with the latter construction. We use some results of Section 5 to help for the construction. We have found a 3-threshold system for 12 or 13 participants with only 11 padlocks, 36 or 39 keys and only 5 additional devices for a total of 33 latches. We give in Table 2, afterwards, a realization of a packing with 3-subsets. Then we proceed by inspection of the triples and pairs of triplets of keys. There are $\binom{13}{3} = 286$ triples of triplets and among them 56 have only

Table 2: Distribution of 11 keys to 13 participants without any reused pair.

Player	1	2	3	4	5	6	7	8	9	10	11	12	13
	1	1	1	1	1	2	2	2	2	3	3	3	3
keys	2	4	6	8	10	4	5	8	9	4	5	8	9
	3	5	7	9	11	6	7	10	11	7	6	11	10

6 distinct keys. All the other triples have at least 7 distinct keys. Also, there are $\binom{13}{2} = 78$ pairs of triplets and among them 24 have exactly 6 distinct keys. All the other pairs have at most 5 distinct keys. Further, on the one hand, all those 24 pairs contain no more and no less than 2 keys among $8, 9, 10, 11$. On the other hand, among the 56 triples either they contain more than 3 keys among $8, 9, 10, 11$ or their 6 distinct keys are lower than 7. This is summarized by Equation (8).

$$\begin{aligned}&(7 \text{ out-of } 1\ldots11) \quad \textbf{OR} \\ &(\ (6 \text{ out-of } 1\ldots11) \quad \textbf{AND} \quad ((3 \text{ out-of } 8\ldots11) \ \textbf{OR} \ (5 \text{ out-of } 1\ldots7))) \end{aligned} \tag{8}$$

So, by luck, the following construction realizes a 3-threshold system for 13 participants with 11 padlocks. We need a 7-out-of-11 device as well as a 6-out-of-11, a 5-out-of-7 and a 3-out-of-4 of our designs. Finally a classical 2-out-of-2 device is needed for the **AND** part. All of these are organized as follows, in order to realize the formula of Equation (8).

Each of the eleven padlocks is used once to close a chain as in Algorithm 2. For each padlock its associated chain will go through the hole of each of up to the four devices (the devices $(7, 11)$ and $(6, 11)$ have each 11 latches so are linked to all the padlock; while device $(5, 7)$ is for the padlocks numbered 1 to 7 and device

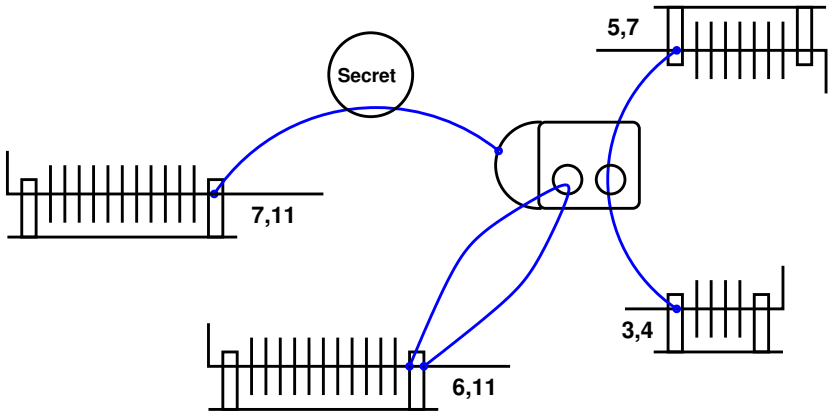

Figure 11: A 3-threshold realization for 13 participants with 11 padlocks. Each participant owns 3 keys with the distribution of Table 2. On the one hand, any 3 participants have either at least 7 distinct keys or if they have only 6 keys then they have at least 5 for padlocks numbered 1 to 7 or at least 3 for padlocks numbered 8 to 11. On the other hand, no pair of participants has a total of 6 distinct keys and either 5 of the first seven ones or 3 for the last four ones.

$(3, 4)$ is for the padlocks numbered 8 to 11). This will realize the disjunctions **OR** in Equation (8). Finally, the disjunction of the devices $(5, 7)$ and $(3, 4)$ is linked via a chain, and that together with the $(6, 11)$ device are associated via a 2-out-of-2 device, as in Algorithm 3. The whole system is shown in Figure 11. Overall, it requires less padlocks, but quite a bunch of other devices.

Remark 22. *Of course the same system works also for a* 3*-threshold realization for* 12 *participants with* 11 *padlocks. Just use the* 12 *first triplets of keys of Table 2 with the same system.*