Updating the Parameters of a Threshold Scheme by Minimal Broadcast

S. G. Barwick[1*], Wen-Ai Jackson[1*] and Keith M. Martin[2]

[1]Department of Pure Mathematics, University of Adelaide
Adelaide 5005, Australia

[2]Information Security Group, Royal Holloway, University of London
Egham, Surrey TW20 0EX, U.K.

Abstract

Threshold schemes allow secret data to be protected amongst a set of participants in such a way that only a pre-specified threshold of participants can reconstruct the secret from private information (shares) distributed to them on system setup using secure channels. We consider the general problem of designing unconditionally secure threshold schemes whose defining parameters (the threshold and the number of participants) can later be changed by using only public channel broadcast messages. In this paper we are interested in the efficiency of such threshold schemes, and seek to minimise storage costs (size of shares) as well as optimise performance in low bandwidth environments by minimising the size of necessary broadcast messages. We prove a number of lower bounds on the smallest size of broadcast message necessary to make general changes to the parameters of a threshold scheme in which each participant already holds shares of minimal size. We establish the tightness of these bounds by demonstrating optimal schemes.

keywords Cryptology, secret sharing schemes, threshold schemes, bounds and constructions.

1 Introduction

Let k and n be integers satisfying $1 \leq k \leq n$. A (k, n)-threshold scheme [3, 16] is a system for sharing a piece of secret information, known as the *secret*, amongst a set $\mathcal{P}$ of n *participants* in such a way that the secret can be reconstructed from any k *shares*, where a share is a private piece of information distributed securely by a trusted *dealer* to each participant on initial setup of the threshold scheme. The *threshold structure* Γ is the collection of subsets of $\mathcal{P}$ whose shares can collectively be used to reconstruct the secret, in other words $\Gamma = \{A \subseteq \mathcal{P} : |A| \geq k\}$. All

*This work was supported by the Australian Research Council

the threshold schemes discussed in this paper are *perfect* in the sense that knowledge of $k-1$ shares contributes no information to knowledge of the secret, and *unconditionally secure* in the sense that the security of the system does not depend on the difficulty of factorization etc.

Threshold schemes are useful cryptographic primitives with many different applications. Examples include access control, protection of a cryptographic key, group signature protocols and controlled key recovery. All these applications have in common the need to distribute trust in a secret parameter amongst a number of different entities. For more details of some applications, see for example [18].

There is a significant communication cost involved in setting up a (k, n)-threshold scheme since the dealer must use secure channels to distribute each participant's share to them. There are many applications where such a one-off cost can be tolerated, but where it is not practical to assume the existence of such secure channels after the setup process has completed. For example, root cryptographic keys are often protected by threshold schemes where shares of the key are distributed manually to participants. This manual distribution process represents a temporary secure channel between the dealer and each participant that may not be practical to reactivate at a later date (the participants might be based in different countries, for example).

This raises the interesting question as to whether it is possible to make changes to the basic parameters of a (k, n)-threshold scheme after the setup process has completed without having to use secure channels. Such a change may be required for a number of reasons: a set of participants might need to be removed from the scheme (*disenrollment*), involving a reduction in n; a set of participants might need to be added to the scheme (*enrollment*), involving an increase in n; the security policy relating to the threshold scheme might need to be strengthened (*threshold increase*), involving an increase in k; or slackened (*threshold decrease*), involving a decrease in k; or indeed any combination of the above.

An impractical solution to this problem would be for the dealer to distribute to each participant at setup not only a share in the original (k, n)-threshold scheme, but also one share in every possible (k', n') threshold scheme that might be required in the future. To change parameters it would suffice that the dealer use a public channel to *broadcast* a message instructing participants to start using the appropriate new shares. However this solution generally requires each participant to store an excessive number of unnecessary shares.

It is therefore desirable to investigate threshold schemes where participants do not hold excessively large shares (we will be interested in them holding shares of minimal size), but where the the dealer can still use a public channel to broadcast some information that enables the threshold scheme parameters to change. Each participant in the "new" threshold scheme can determine their share exclusively from the information that they received on system setup and the broadcast message. We assume that the dealer anticipates that a future parameter change may be necessary before issuing the initial shares. This allows the dealer to build the capability for parameter change into the threshold scheme at setup. Without this assumption there are only a few types of parameter change that can be enabled using only broadcast channels (see Section 5).

The schemes that we look at will vary depending on the amount of knowledge that the dealer has about what future parameter changes will be needed. For reasons that we make clear in Section 3, the following three cases are of particular interest:

- The dealer anticipates that the threshold may decrease (but not by how much) and that some participants may need to be disenrolled (but does not know how many).
- The dealer anticipates that the threshold may increase (but not by how much) and that some participants may need to be disenrolled (but does not know how many).
- The dealer anticipates that the threshold may change (but does not know whether it will increase or decrease) and that some participants may need to be disenrolled (but does not know how many).

Threshold schemes capable of changing their parameters within the same communications network context as this paper have been studied by a number of authors. A lower bound on the necessary share size to enable sequential disenrollment of participants in a threshold scheme was given in [4]. Both [4] and [14] demonstrated the optimality of this bound by providing different threshold schemes that met this lower share bound. In [5] a framework was provided for studying this problem for secret sharing schemes (a generalisation of threshold schemes) and the lower bound on share size proved in [4] was generalised for this environment.

We are interested in not just minimising the share size, but also the necessary broadcast information to enable a change in the parameters of a threshold scheme. In [2] a lower bound was shown for the amount of broadcast information necessary in the sequential disenrollment schemes of [4, 14]. In this paper we significantly extend this work by looking at general parameter changes for threshold schemes. In particular we will provide lower bounds on the size of broadcast message necessary to enable any type of meaningful change to the parameters of a threshold scheme that already has minimal share size. The following is a simplified version of our main theorem (Theorem 11).

Theorem Consider a (k, n)–threshold scheme with $k < n$ on a participant set $\mathcal{P}$ with a secret s to be updated via a broadcast to Γ', any (k', n')–threshold access structure with secret s' on a subset of $\mathcal{P}$. Let $b_{\Gamma'}$ be the associated broadcast. Suppose that each participant p holds a share of minimal size (that is, $H(p) = 2H(s) = 2H(s')$). Then the size $H(b_{\Gamma'})$ of the broadcast $b_{\Gamma'}$ satisfies

$$H(b_{\Gamma'}) \geq \begin{cases} (\min(n-1, n') - k' + 1)H(s) & \text{if } k' \geq k \text{ and } n' \leq n \\ (n' - k' + 1)H(s) & \text{if } k' \leq k \text{ and } n' \leq n \text{ and } k - k < n - n' \\ (\min(k, n') - k' + 1)H(s) & \text{if } k' \leq k \text{ and } n' \leq n \text{ and } k - k \geq n - n'. \end{cases}$$

We also show that these bounds are optimal by exhibiting schemes that meet these bounds.

Note that our communications environment differs from the one on which the *redistribution* techniques of [7, 9, 15] can be used to change the parameters of a threshold scheme. In redistribution environments there is no secure channel from the dealer to the participants to enable parameter change, but there do exist secure channels between the participants themselves. We make no such assumption here. The problem under discussion here is also related, but different, to the concept of *proactive* threshold schemes [10], where broadcast messages are used to refresh shares, but not to change the parameters of the threshold scheme.

The remainder of the paper is structured as follows. In Section 2 we introduce the necessary preliminary concepts about threshold schemes. In Section 3 we present the model we use and discuss the methodology of the paper. In Sections 4, 5 and 6 we consider three different types of parameter change and establish lower bounds on the broadcast size for share-minimal threshold schemes enabling such changes to be made. We establish the optimality of these bounds in Section 7 by demonstrating optimal constructions of dynamic threshold schemes. In Section 8 we discuss two possible avenues for further work. Appendix A contains a brief introduction to the standard entropy notation and results. Finally, for easier readability, all the technical proofs of results stated in Sections 4, 5 and 6 have been placed in Appendix B.

2 Preliminaries

Since the threshold schemes that we discuss here are *unconditionally secure* (their security is independent of cryptographic assumptions on the strength of an adversary) we follow the popular convention (first proposed by [13]) of modeling them in information theoretic terms. See Appendix A for a short introduction to the necessary information theory and the notation used. We will formally define a threshold scheme within this context.

For ease of translation from sets to random variables, throughout this paper we adopt the following conventions: if A and B are finite sets then we simplify $A \cup B$ to AB and the singleton set $\{x\}$ to x (hence $s\mathcal{P}$ represents the set $\{s\} \cup \mathcal{P}$ etc.).

2.1 Threshold Schemes

Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a set of participants, let s be the secret, and let k be an integer with $1 \leq k \leq n$.

Definition 1 A (k, n)-*threshold scheme* $\mathcal{M} = (s\mathcal{P}, \rho)$ is a probability distribution ρ defined on a collection of tuples $\langle s\mathcal{P} \rangle$, each of which is indexed by the elements of $s\mathcal{P}$, such that for $A \subseteq \mathcal{P}$,

$$H(s \mid A) = \begin{cases} 0 & \text{if } |A| \geq k \\ H(s) & \text{if } |A| \leq k-1. \end{cases}$$

We call the elements of $[s\mathcal{P}]$ *distribution rules.* In order to implement a threshold scheme, the collection $[s\mathcal{P}]$ of distribution rules is made public. A dealer privately selects a distribution rule $\pi = (x_s, x_1, \ldots, x_n)$ with probability $\rho(\pi)$, then securely distributes x_i as a share to p_i, for $i = 1, \ldots, n$. The element x_s is the secret, and is kept private.

We call $H(p_i)$ the *size* of the share associated with participant p_i, and $H(s)$ the *size* of the secret. It can be seen (for example [19]) that in any threshold scheme, $H(p_i) \geq H(s)$. If $H(p_i) = H(s)$ for all such p_i then we say that the threshold scheme is *ideal.* Ideal (k, n)-threshold schemes can be found for all integers $1 \leq k \leq n$. We describe two examples that are used in Section 7.

Example 2 (Shamir[16]) Let $\mathcal{P} = \{p_1, \ldots, p_n\}$, let p be a prime and let $\mathcal{Z}_p$ be the field of integers modulo p. Suppose k is an integer with $2 \leq k \leq n \leq p$. A dealer generates distinct, non-zero elements $x_1, \ldots, x_n$ of $\mathcal{Z}_p$ and publishes them. The dealer then secretly and randomly chooses elements $a_0, a_1, \ldots, a_{k-1} \in \mathcal{Z}_p$ and forms the polynomial $a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1}x^{k-1}$. For $i = 1, \ldots, n$, the share $a(x_i)$ is issued to participant p_i and the value of the secret is a_0. It is straightforward to verify that any k participants can determine a_0 by polynomial interpolation, but any $k-1$ participants can obtain no information about the value of a_0, additional to the fact that it is in $\mathcal{Z}_p$. In this case there are p^k distribution rules $(a(0), a(x_1), \ldots, a(x_n))$ in $[s\mathcal{P}]$, corresponding to the p^k values of the k-tuple $(a_0, a_1, \ldots, a_{k-1})$. Since ρ is uniform we have that $H(p_i) = H(s) = \log p$ and thus that the scheme is ideal.

Example 3 An equivalent way to construct an ideal (k, n)-threshold scheme uses a geometric construction in $\Sigma = \mathrm{PG}(k-1, q)$ (for a background in projective geometry see [11]). Let $\sigma\colon s\mathcal{P} \to \Sigma$ be a mapping that assigns to each participant p_i as share a point p_i^σ on a normal rational curve in Σ and assigns the secret s to be a further point s^σ on this curve. If k participants pool their shares, these shares span Σ and so they can obtain the secret. If $k-1$ participants pool their shares, these shares span a $(k-2)$-dimensional subspace which contains no further point of the normal rational curve, so in particular does not contain s^σ. They thus have no information about the secret $s = s^\sigma$. To see how to extract the distribution rules of an ideal (k, n)-threshold scheme from this configuration of points see for example [19].

2.2 Restrictions and Contractions

In order to define our model rigorously, we will make use of two types of threshold schemes that can be derived from an existing threshold scheme. The *restriction* of a (k, n)-threshold scheme to a subset of n' participants is the (k, n')-threshold scheme that results from effectively discarding the shares held by the other $n - n'$ participants. The *contraction* of a (k, n)-threshold scheme at a set of r shares is the $(k-r, n-r)$-threshold scheme that results from effectively broadcasting this set of r shares.

More generally, let ρ be a probability distribution on a finite collection $\langle X \rangle$ of tuples indexed by the finite set X. For $A \subseteq X$, the *restriction to* A of the pair (ρ, X) is the pair (ρ_A, A). For $B \subseteq X$ and $A = X \setminus B$, the *contraction at* $B = \beta \in [B]$ of the pair (ρ, X) is the pair $(\rho_{A|B=\beta}, A)$. Restrictions and contractions of threshold schemes are formalised by the following two results from [12].

Theorem 4 (Restriction) [12] *Let $\mathcal{M} = (s\mathcal{P}, \rho)$ be a (k, n)-threshold scheme and let $\mathcal{P}' \subseteq \mathcal{P}$. Then $\mathcal{M}' = (s\mathcal{P}', \rho_{s\mathcal{P}'})$ is a $(k, |\mathcal{P}'|)$-threshold scheme, known as the restriction of $\mathcal{M}$ to $s\mathcal{P}'$.*

Theorem 5 (Contraction) [12] *Let $\mathcal{M} = (s\mathcal{P}, \rho)$ be a (k, n)-threshold scheme. Let $B \subseteq \mathcal{P}$, let $\mathcal{P}' = \mathcal{P} \setminus B$ and let $\beta \in [B]$. Then $\mathcal{M}' = (s\mathcal{P}', \rho_{s\mathcal{P}'|B=\beta})$ is a $(k - |B|, |\mathcal{P}'|)$-threshold scheme, known as the contraction of $\mathcal{M}$ at $B = \beta$.*

3 Dynamic Threshold Schemes

In this paper we are interested in threshold schemes where the parameters can later be changed by means of a public channel broadcast. In this section we first comment on the special case of enrollment. We then propose a simple extension of the model of a threshold scheme within which to analyse dynamic threshold schemes.

3.1 Enrollment

There is one type of parameter change that can not be easily accommodated in the communication network environment that we propose. Enrollment of new participants who were not issued with any private information at system setup is impossible in a broadcast only network. The reason for this is that each new participant needs to acquire some private information from the dealer, which clearly needs the involvement at some stage of a secure distribution channel. The only ways in which enrollment could be performed are:

- A secure channel is set up between the dealer and any new enrolling participants to issue them with shares.
- All possible future participants are issued with a cryptographic key at system setup. These participants are then effectively "sleeping participants" until the time of enrollment, when the dealer broadcasts their share to them, encrypted under the key that they were issued at setup. This is essentially the same technique used in [17] to remotely activate threshold schemes.
- Existing participants transfer necessary information using secure channels to new enrolling participants (this is outside our communications model, but is appropriate in the redistribution environments mentioned in Section 1).

For this reason we do not consider enrollment in the rest of this paper, and acknowledge that if enrollment is required then secure channels must be established using one of the above techniques.

3.2 A Model for Dynamic Threshold Schemes

Let $\mathcal{P}$ be a set of participants and s be a secret. Let $\mathcal{U}$ be a collection of threshold structures defined on subsets of $\mathcal{P}$ (in other words, for each $\Gamma' \in \mathcal{U}$ there exist k', n' and $\mathcal{P}' \subseteq \mathcal{P}$ such that Γ' is a (k', n')-threshold structure defined on $\mathcal{P}'$).

We wish to establish a (k, n)-threshold scheme defined on $\mathcal{P}$ that has the capability of being changed by means of a broadcast message into a scheme with threshold structure Γ', where Γ' can be any of the threshold structures in $\mathcal{U}$. We denote the secret after this change by s'. There is no logistical reason for s and s' to be different, but we will see that for many parameter changes they are necessarily independent. We thus make the reasonable assumption throughout that

$$H(s) = H(s'). \tag{1}$$

Each $\Gamma' \in \mathcal{U}$ is associated with a *broadcast variable* $b_{\Gamma'}$, which represents the broadcast message that the dealer will send if he wishes to change to the threshold structure Γ'. We let $\mathcal{B} = \{b_{\Gamma'} | \Gamma' \in \mathcal{U}\}$.

Definition 6 A (k,n)*-threshold scheme* $\mathcal{M} = (\rho, ss'\mathcal{PB})$ *that can be updated to* $\mathcal{U}$, is a probability distribution ρ defined on a collection of tuples $\langle ss'\mathcal{PB}\rangle$ (each of which is indexed by the elements of $ss'\mathcal{PB}$) such that:

(A) $\mathcal{M}$ restricted to $s\mathcal{P}$ is a (k,n)-threshold scheme on $\mathcal{P}$ with secret s, that is,

$$H(s \mid A) = \begin{cases} 0 & \text{if } |A| \geq k \\ H(s) & \text{if } |A| \leq k-1 \end{cases};$$

(B) For each threshold structure $\Gamma' \in \mathcal{U}$, if Γ' is a (k',n')-threshold structure on $\mathcal{P}'$ then $\mathcal{M}$ contracted at $b_{\Gamma'} = \beta \in [b_{\Gamma'}]$ is a (k',n')-threshold scheme on $\mathcal{P}'$ with secret s', that is,

$$H(s' \mid Ab_{\Gamma'}) = \begin{cases} 0 & \text{if } |A \cap \mathcal{P}'| \geq k' \\ H(s') & \text{if } |A \cap \mathcal{P}'| \leq k'-1 \end{cases}.$$

In other words, $\mathcal{M}$ is initially a (k,n)-threshold scheme. If the broadcast message $b_{\Gamma'}$ is sent on a public channel then knowledge of the original shares and this broadcast result in $\mathcal{M}$ also becoming a (k',n')-threshold scheme defined on $\mathcal{P}'$.

Note that in Definition 6 we do not care whether a set of participants belonging to Γ' can obtain s' prior to knowledge of the broadcast $b_{\Gamma'}$. It is foreseen that in most anticipated applications that s' will not have any relevant meaning until the point at which the dealer initiates a parameter change (for example, s' may be the backup master key that the dealer will only activate in the event that a parameter change is necessary).

We are interested firstly in minimising the size of shares held by each participant, which is measured by $H(p)$. We are then interested in minimising the size of the broadcast $b_{\Gamma'}$, which is measured by $H(b_{\Gamma'})$. In this paper, for a number of different sets $\mathcal{U}$, we will determine the minimal size of broadcast necessary in a share minimal threshold scheme that can be updated to $\mathcal{U}$. Whereas lower bounds on share size are easily extracted from existing work and tend to be "expected", lower bounds on broadcast size are neither established nor particularly intuitive. For example, it would seem intuitive that broadcast size should depend on the set $\mathcal{U}$, and that larger sets $\mathcal{U}$ will require larger broadcasts, but we prove the slightly surprising result that the minimal broadcast size is "fairly independent" of $\mathcal{U}$.

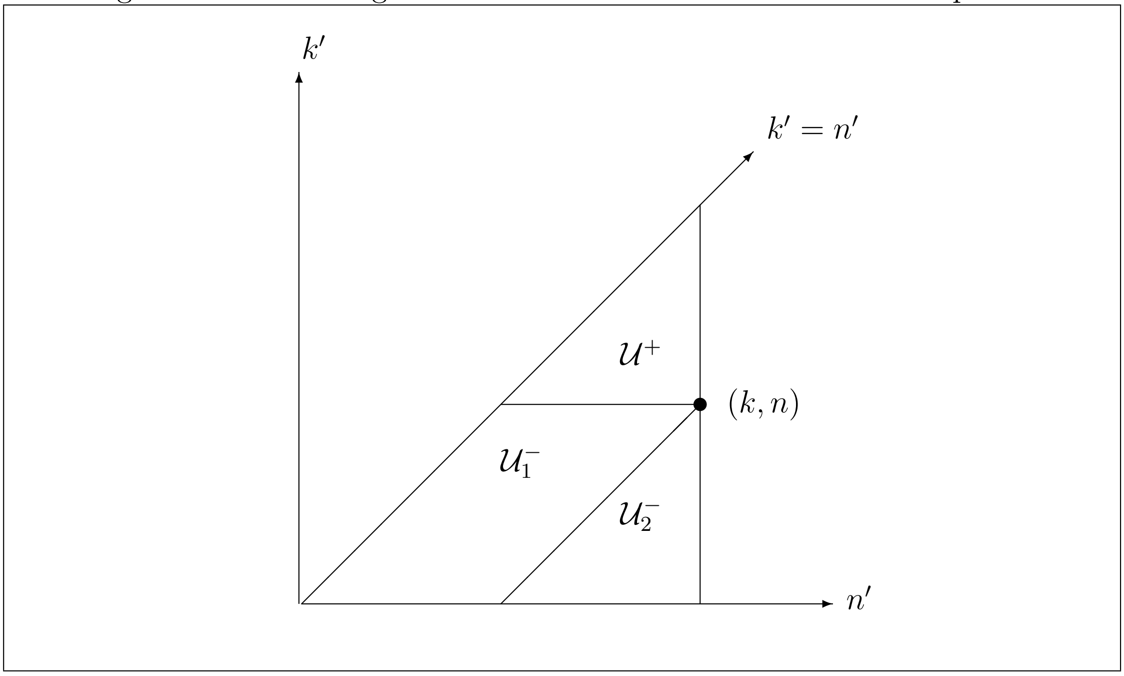
We proceed by identifying some "sensible" sets $\mathcal{U}$ to study. First observe that if a lower bound holds for updating to $\mathcal{U}$ then it also holds for updating to any region $\mathcal{U}' \supseteq \mathcal{U}$. We thus identify some meaningful "large" regions $\mathcal{U}$ to investigate, and in Section 6.2 will later show that updating to "smaller" regions generally does not result in smaller broadcast sizes.

The three main regions $\mathcal{U}$ that we study are:

1. *Threshold increases.* The dealer wants it to be possible to change to any threshold structure with a greater threshold parameter. In other words, all (k',n')-threshold structures with $k' \geq k$ and $n' \leq n$. We denote this set by $\mathcal{U}^+(k,n)$, or $\mathcal{U}^+$ when no ambiguity arises.

2. *Threshold decreases.* The dealer wants it to be possible to change to any threshold structure with a smaller threshold parameter. In other words, all (k',n')-threshold structures with $k' \leq k$ and $n' \leq n$. We denote this set by $\mathcal{U}^-(k,n)$, or simply $\mathcal{U}^-$. For reasons that will later be explained we partition $\mathcal{U}^-$ into $\mathcal{U}_1^-$ (corresponding to $k-k' < n-n'$) and $\mathcal{U}_2^-$ (corresponding to $k-k' \geq n-n'$).

Figure 1: Selected regions to which threshold schemes can be updated



3. *The general case.* The dealer wants it to be possible to change to any (k', n')-threshold structure with $n' \leq n$. We denote this set by $\mathcal{U}^T(k,n)$, or simply $\mathcal{U}^T$. Clearly $\mathcal{U}^T = \mathcal{U}^+ \cup \mathcal{U}^- = \mathcal{U}^+ \cup \mathcal{U}_1^- \cup \mathcal{U}_2^-$.

An example of a smaller region of interest is where $k' = k$ and $n' \leq n$ (this corresponds to disenrollments). We return to this is Section 6.2. The listed regions are illustrated in Figure 1.

In the following sections we look at these different regions in turn and determine lower bounds on the broadcast size for updating to them. In Section 4 we look at $\mathcal{U}^+$, in Section 5 we look at $\mathcal{U}^-$, and in Section 6 we look at $\mathcal{U}^T$ as well as discussing the possibility of improving these results for smaller update regions.

4 Increasing the threshold

In this section we consider the case of increasing the threshold, that is, we look at updating to threshold structures in $\mathcal{U}^+$. We first need to establish exactly what the minimal share size is for this case.

Theorem 7 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a (k,n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^+$. Then*

(a) *s and s' are independent*

(b) *for each participant $p \in \mathcal{P}$, $H(p) \geq 2H(s)$.*

The proof of this is not difficult, and appears in Appendix B. We thus refer to a (k,n)-threshold scheme that can be updated to $\mathcal{U}^+$ and has $H(p) = 2H(s)$ for all $p \in \mathcal{P}$ as *share minimal.*

Theorem 8 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a share minimal (k,n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^+(k,n)$. Then for any $\Gamma' \in \mathcal{U}^+(k,n)$, where Γ' is a (k',n')-threshold structure,*

$$H(b_{\Gamma'}) \geq \begin{cases} (n'-k'+1)H(s) & \text{if} \quad n' < n \\ (n'-k')H(s) & \text{if} \quad n' = n. \end{cases}$$

The complete proof of this theorem is complex, see Appendix B for full details. We sketch the proof here to provide an idea of how it works. Theorem 8 is proved by induction on k. We first prove the result for $k = 1$, that is, Γ is a $(1,n)$ threshold scheme and $H(p) = 2H(s) = 2H(s')$. We derive two parts from $\mathcal{M}$, one part relating to Γ and the other relating to $\Gamma' \in \mathcal{U}^+(1,n)$. We then find entropy results concerning the participants, the broadcasts and s (see Lemmas 17 and 18 in Appendix B). Using these results we can prove the size of the broadcast for $k = 1$ (see Lemma 19 in Appendix B). To prove the result for general k, we assume that $k > 1$, we contract on a $k-1$ subset of $\mathcal{P}$ to obtain a $(1, n-(k-1))$ threshold scheme that can be updated to $\mathcal{U}^+(1, n-(k-1))$ for an appropriate choice of broadcast. Now we apply the result for the case $k = 1$ and Theorem 8 follows.

We will see in Section 7 that this bound is tight when we demonstrate a share minimal scheme that also has minimal broadcast size.

Recall that, as discussed immediately after Definition 6, our model is not concerned with whether participants belonging to Γ' can obtain s' prior to knowledge of the broadcast $b_{\Gamma'}$. It is worth observing that if the model is restricted to make the extra requirement that they cannot obtain s', we get the simplified bound $H(b_{\Gamma'}) \geq (n'-k'+1)H(s)$.

5 Decreasing the threshold

In this section we consider decreasing the threshold. We wish to establish a lower bound on the broadcast size necessary for a share minimal (k,n)-threshold scheme that can be updated to $\mathcal{U}^-$.

This case is interesting because there are a number of parameter sets within this region that any standard threshold scheme can be updated to, without the need for extra share information on scheme initialisation. This partitions $\mathcal{U}^-$ into two separate regions $\mathcal{U}_1^-$ and $\mathcal{U}_2^-$, where $\mathcal{U}_1^-$ corresponding to all (k',n') pairs where $k-k' < n-n'$, and $\mathcal{U}_2^-$ corresponds to all (k',n') pairs where $k-k' \geq n-n'$.

We will first discuss a special case arising as a result of this issue and then deal with the two separate regions.

5.1 A special case: $k = n$

The region $\mathcal{U}_2^-$ is interesting because it is possible to update any standard (k, n)-threshold scheme to a (k', n')-threshold scheme in $\mathcal{U}_2^-$ by broadcasting some selected share information that allows remaining participants to continue using their original shares within a new scheme. A simple example would be the fact that broadcasting the share held by any participant effectively converts the original scheme into a (k', n')-threshold scheme, with that participant "removed". In such schemes there is no need to distribute extra share information and so $H(p) \geq H(s)$.

However, the region $\mathcal{U}_2^-$ is otherwise artificial and providing the general capability of decreasing the threshold normally involves the inclusion of (k', n') pairs outside this region, except in one significant case. When $k = n$, we have $\mathcal{U}_1^- = \emptyset$ and $\mathcal{U}_2^- = \mathcal{U}^-$. This special case was studied in [1], where it was shown that for schemes with the minimal share size of $H(p) = H(s)$, the minimal broadcast size is $H(b_{\Gamma'}) = \min(k - k', n' - k' + 1)H(s)$. We refer the reader to [1] for details, and for examples of schemes with this minimal broadcast size.

5.2 Decreasing the threshold when $k < n$

For the rest of this section we thus only consider the case $k < n$. We first establish that in contrast to the special case $k = n$, when $k < n$ the size of shares in a (k, n)-threshold scheme that can be updated to $\mathcal{U}^-$ is at least $2H(s)$.

Theorem 9 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a (k, n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^-$. Then $H(p) \geq 2H(s)$.*

As in Section 4 we refer to a scheme with the minimal share size of $H(p) = 2H(s)$ for all $p \in \mathcal{P}$ as *share minimal.* The main result of this section is the following.

Theorem 10 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a share minimal (k, n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^-$. Then for any $\Gamma' \in \mathcal{U}^-$, where Γ' is a (k', n')-threshold structure,*

$$H(b_{\Gamma'}) \geq \begin{cases} (n' - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}_1^- \\ (\min(k, n') - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}_2^-. \end{cases}$$

The complete proofs are in Appendix B, but we comment on them here. We have already seen that the two regions $\mathcal{U}_1^-$ and $\mathcal{U}_2^-$ are in some respects fundamentally different. In fact, to prove a lower bound on the broadcast size for updating to $\mathcal{U}^-$ we need two different approaches for each of these two regions. The method of proof for the region $\mathcal{U}_1^-$ is similar to that of Theorem 8. The proof for the region $\mathcal{U}_2^-$ involves the following series of steps. The first step is to show that, for $A \subseteq \mathcal{P}$ with $|A| \leq k$, $H(A) = 2|A|H(s)$ and that for any $A \subseteq P$, $H(A) = (\min(k, |A|) + |A|)H(s)$. This is proved by induction on k. The next step is to prove that $H(b_{\Gamma'}) \geq \min(k, n')H(s)$ if Γ' is a $(1, n')$ threshold structure in $\mathcal{U}_2^-(k, n)$. The final step is to prove the result for $\Gamma' \in \mathcal{U}_2^-(k, n)$ by using induction on k.

6 Updating to other regions

We have demonstrated lower bounds on the broadcast size of share minimal threshold schemes that can be updated to have lower, or higher threshold parameters. In this section we briefly consider the general case, where the threshold can be either increased or decreased, and then discuss updating to smaller regions.

6.1 Updating the threshold to $\mathcal{U}^T$

By Theorems 7 and 9 it follows that any (k, n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^T$ has $H(p) \geq 2H(s)$ for all $p \in \mathcal{P}$. The following is immediate from Theorems 8 and 10.

Theorem 11 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a share minimal (k, n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^T$. Then for any $\Gamma' \in \mathcal{U}^T$, where Γ' is a (k', n')-threshold structure,*

$$H(b_{\Gamma'}) \geq \begin{cases} (\min(n-1, n') - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}^+ \\ (n' - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}_1^- \\ (\min(k, n') - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}_2^- . \end{cases}$$

We show in Section 7 that this lower bound is tight by providing a scheme that meets it.

6.2 Updating to smaller regions

We have already established results for updating to the regions $\mathcal{U}^+$, $\mathcal{U}^-$ and $\mathcal{U}^T$. Recall that, as remarked in Section 3.2, it is possible that these bounds might be able to be reduced if we only want to update to smaller regions.

The main problem with studying smaller regions is simply that it is not obvious which smaller regions might be of interest in genuine applications. Table 1 gives some examples of "sensible" smaller regions $\mathcal{U}$. In general they show that so long as the update region is reasonably large then it is not possible to have a share minimal (k, n)-threshold scheme that can be updated to $\mathcal{U}$ using a smaller broadcast message than the bound of Theorem 11. The proofs of most of these bounds are not provided here as they can either be derived from the proofs of results in previous sections, or can be derived in a similar manner.

A few of these cases however do deserve special mention. Case 1 corresponds to the sequential disenrollment schemes studied in [2, 4, 14]. In this case, considering only one disenrollment, because only one participant will ever be removed from the scheme it is possible to have a small broadcast size. Case 5 ($\mathcal{U} = \mathcal{U}_2^-$) and Case 6 are of interest because the conditions for Lemmas 14 and 15 of Appendix B do not apply. In these cases it is possible to design schemes for updating to $\mathcal{U}$ where $s = s'$ and $H(p) = H(s)$ for all $p \in \mathcal{P}'$. The broadcast bound indicated in Table 1 is only one less than that of Theorem 11, and only when $k < n'$. These cases, and proofs of their broadcast bounds, are given in [1] (see also Section 5.1).

Case	$\mathcal{U}$ *defined by* k'	n'		*Minimum share size*	*Broadcast lower bound:* $H(b_{\Gamma'}) \geq$
1	$k' = k$	$n' = n - 1$		$2H(s)$	$H(s)$
2	$k' = k$	$n' < n$		$2H(s)$	$(n' - k' + 1)H(s)$
3	$k' \geq k$	$n' < n$		$2H(s)$	$(n' - k' + 1)H(s)$
4	$k' \leq k$	$n' \leq n$	$k - k' < n - n'$	$2H(s)$	$(n' - k' + 1)H(s)$
5	$k' \leq k$	$n' \leq n$	$k - k' \geq n - n'$	$H(s)$	$\min(k - k', n' - k' + 1)H(s)$
6	$k' < k$	$n' = n$		$H(s)$	$\min(k - k', n' - k' + 1)H(s)$

Table 1: Share and broadcast bounds for updating to some smaller regions $\mathcal{U}$

7 A Construction

We now demonstrate that the bound on the broadcast size of Theorem 11 (and thus also the bounds of Theorems 8 and 10) is tight by constructing a share-minimal (k, n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^T$ with the minimal broadcast size indicated by Theorem 11.

We first indicate the idea behind the construction by demonstrating an extended version of the Shamir threshold scheme (recall Example 2 of Section 2.1) that meets the broadcast bound in some, but not all, cases. We then present a construction based on Example 3 of Section 2.1 that meets the bound of Theorem 11 in all cases.

Example 12 We divide the scheme into three phases:

Initialisation: The dealer issues each participant p_i in $\mathcal{P} = \{p_1, \ldots, p_n\}$ with a share in each of two Shamir threshold schemes, both defined on $\mathcal{P}$ and $n - 1$ 'imaginary' shareholders $f_1, \ldots, f_{n-1}$. Scheme I is a $(k, 2n - 1)$-threshold scheme with secret s and Scheme II is an $(n, 2n - 1)$-threshold scheme with secret s'. Let $a(x)$ and $a'(x)$ be the polynomials corresponding to Scheme I and Scheme II respectively. The dealer generates distinct non-zero values $x_1, \ldots, x_n, y_1, \ldots, y_{n-1}$ in $\mathcal{Z}_p$ and publishes these. Each participant p_i is given share $(a(x_i), a'(x_i))$.

Before update: Participants can use their shares of Scheme I to realise a (k, n)-threshold scheme.

Update: Suppose that we wish the scheme to be updated to $\Gamma' \in \mathcal{U}^T$, a (k', n')-threshold structure on $\mathcal{P}' = \{p_1, \ldots, p_{n'}\}$. That is, we want to disenroll participants $p_{n'+1}, \ldots, p_n$ and change the threshold parameter to k'. In order to activate Γ', the dealer has two options:

1. The dealer indicates that participants should switch to using their shares in Scheme II and broadcasts $a'(x_{n'+1}), \ldots, a'(x_n), a'(y_1), \ldots, a'(y_{n'-k'})$. Any k' participants in $\mathcal{P}'$ who pool their shares with the $n - k'$ broadcast shares know n points on polynomial $a'(x)$ of degree $n - 1$, so can uniquely determine $a'(x)$ and obtain $s' = a'(0)$. However, any $k' - 1$ participants in $\mathcal{P}'$ knowing the broadcast shares only have $n - 1$ points on $a'(x)$ and so obtain no information about s'. The result of the broadcast is thus a (k', n')-threshold scheme on $\mathcal{P}'$. The broadcast has size $H(b_{\Gamma'}) = (n - k')H(s)$, which only meets the bound of Theorem 11 in a few cases (for example when $n' \geq n - 1$ and $k' \geq k$).

2. In the special case that $\Gamma' \in \mathcal{U}_2^-$, the dealer broadcasts the values $a'(0) - a(0)$ and $a(x_{n'+1}), \dots, a(x_n), a(y_1), \dots, a(y_{(k-k')-(n-n')})$. Any k' participants in $\mathcal{P}'$ who pool their shares with the $k - k'$ broadcast shares know k points on polynomial $a(x)$ of degree $k - 1$, so can determine $s = a(0)$ and hence, also knowing $a'(0) - a(0)$, can determine $a'(0)$. Similarly, any $k' - 1$ participants obtain no information about s'. In this case the broadcast has size $(k - k' + 1)H(s)$, which meets the bound in Theorem 11 only if $k \leq n'$.

Example 12 only meets the bound of Theorem 11 for some parameters. We now give a general geometric construction based on Example 3 that meets the bound in all cases.

Example 13 The scheme is divided into three phases:

Initialisation: The dealer issues each participant p_i in $\mathcal{P} = \{p_1, \dots, p_n\}$ with a share in each of two geometric threshold schemes, defined as follows.

1. Let $F = \{f_1, \dots, f_{k-1}\}$ be a set of "imaginary" participants. Denote $\Sigma = \mathrm{PG}(k-1, q)$ and let $\sigma\colon s\mathcal{P}F \to \Sigma$ be a geometric $(k, n+k-1)$-threshold scheme.
2. Let $H = \{h_1, \dots, h_{n-1}\}$ be a set of "imaginary" participants. Denote $\Sigma' = \mathrm{PG}(n-1, q)$ and let $\sigma'\colon s'\mathcal{P}H \to \Sigma'$ be a geometric $(n, 2n-1)$-threshold scheme.

The two shares held by each participant can be represented as a single subspace by embedding Σ and Σ' as disjoint subspaces in $\Theta = \mathrm{PG}(k+n-1, q)$ and considering the share of participant $p \in \mathcal{P}$ to be the subspace $\langle p^\sigma, p^{\sigma'} \rangle$ of Θ.

Before update: Participants can use their shares of σ to realise a (k, n)-threshold scheme.

Update: Suppose that we wish the scheme to be updated to $\Gamma' \in \mathcal{U}^T$, a (k', n')-threshold structure on $\mathcal{P}' = \{p_1, \dots, p_{n'}\}$. In order to activate Γ', the dealer has two options:

1. Define subspaces $C' = \langle (s'\mathcal{P}')^{\sigma'} \rangle$ and $D' = \langle (\mathcal{P} \setminus \mathcal{P}')^{\sigma'}, h_1^{\sigma'}, \dots, h_{n'-k'}^{\sigma'} \rangle$ of Σ'. In order to activate Γ', the dealer broadcasts the subspace $B' = C' \cap D'$ by choosing a suitable set of $(\dim B' + 1)$ points of B'. As $\langle C', D' \rangle = \Sigma'$, we have

$$\begin{aligned}\dim B' &= \dim C' + \dim D' - \dim\langle C', D' \rangle \\ &= \min(n', n-1) + (n - k' - 1) - (n-1) \\ &= \min(n', n-1) - k'.\end{aligned}$$

   If a set K of k' participants in $\mathcal{P}'$ pool their shares, then $K^{\sigma'}$ is a subspace of dimension $k' - 1$ of C' which, by the properties of a normal rational curve, is disjoint from D' and hence B'. Thus B' and $K^{\sigma'}$ together span C', which contains $s'^{\sigma'}$, so the participants in K can obtain the secret s'.

   For a set L of $k' - 1$ participants we consider the set $X = \langle L^{\sigma'}, D' \rangle$. As $B' \subseteq D'$, it follows that $B' \subseteq X$. The set X is generated by points of the normal rational curve, hence $\dim X = (k' - 1) + ((n - n') + (n' - k')) - 1 = n - 2$. By the properties of a normal rational curve, X does not contain any further point of the normal rational curve, so in particular does not contain s'. This implies that a maximal unauthorised $(k'-1)$-set $L \subseteq \mathcal{P}'$ together with the participants $\mathcal{P} \setminus \mathcal{P}'$ and broadcast B' cannot obtain s'. The result of the broadcast is thus a (k', n')-threshold scheme on $\mathcal{P}'$. We refer to this construction process as *updating with* σ'. If $n' = n$ then $H(b_{\Gamma'}) = (n - k')H(s)$. If $n' < n$ then $H(b_{\Gamma'}) = (n' - k' + 1)H(s)$. So, updating with σ' achieves the bound of Theorem 11 in the following cases: (a) $\Gamma' \in \mathcal{U}^+ \cup \mathcal{U}_1^-$; (b) $\Gamma' \in \mathcal{U}_2^-$ and $n' < k$.

2. For the remaining case, that is $\Gamma' \in \mathcal{U}_2^-$ and $k \leq n'$, we describe a similar process referred to as *updating with* σ. Although we show this for all $\Gamma' \in \mathcal{U}_2^-$, it is only optimal for $k \leq n'$. Define subspaces $C = \langle (s\mathcal{P}')^\sigma \rangle$ and $D = \langle (\mathcal{P} \setminus \mathcal{P}')^\sigma, f_1^\sigma, \ldots, f_{(k-k')-(n-n')}^\sigma \rangle$ of Σ. In order to activate Γ', the dealer broadcasts the subspace $B = C \cap D$, where

$$\begin{aligned}\dim B &= \dim C + \dim D - \dim\langle C, D\rangle \\ &= \min(n', k-1) + (k - k' - 1) - (k-1) \\ &= \min(n', k-1) - k'\end{aligned}$$

and also a point W on the line $\langle s^\sigma, s'^{\sigma'} \rangle$ in Σ^T, where $W \notin \{s^\sigma, s'^{\sigma'}\}$. This gives a (k', n')-threshold scheme on $\mathcal{P}'$ with secret s' and with broadcast satisfying

$$H(b_{\Gamma'}) = (\dim B + 1) + 1 = \min(n', k-1) - k' + 2.$$

Thus for the case $\Gamma' \in \mathcal{U}_2^-$ and $k \leq n'$, updating with σ meets the bound of Theorem 11.

Hence we have shown that the bound in Theorem 11 can always be met by either updating with σ' or updating with σ. Note also that if we wanted to make the assumption that the participants cannot determine s' before the broadcast then we would need σ' to be an $(n+1, 2n)$-threshold scheme, in which case we would have

$$H(b_{\Gamma'}) = \begin{cases} (k - k' + 1)H(s) & \text{if } \Gamma' \in \mathcal{U}_2^- \text{ and } k < n' \\ (n' - k' + 1)H(s) & \text{otherwise.} \end{cases}$$

8 Concluding Remarks

We have established the minimal broadcast necessary to update the parameters of a share-minimal threshold scheme, and demonstrated an optimal scheme for achieving these bounds. We showed these results for achieving one parameter update. A natural question to consider is the situation where we want more than one, say two updates. If Γ on $\mathcal{P}$ is updated to Γ' on $\mathcal{P}' \subseteq \mathcal{P}$ (using $b_{\Gamma'}$), then updated to Γ'' on $\mathcal{P}''$ (using $b_{\Gamma''}$), we would need $\mathcal{P}'' \subseteq \mathcal{P}'$. So we would need to add the extra condition:

$$H(s'' \mid A b_{\Gamma'} b_{\Gamma''}) = \begin{cases} 0 & \text{if } |A \cap \mathcal{P}''| \geq k'', \\ H(s'') & \text{if } |A \cap \mathcal{P}''| \leq k'' - 1. \end{cases}$$

The next step would be to investigate the independence of the secrets s, s' and s''. Under what circumstances would it hold that $H(s'' \mid ss') = H(s'')$?

Thirdly, for which access structures Γ and update collections $\mathcal{U}$ (containing Γ') and $\mathcal{U}''$ (containing Γ'') do we need to have $H(p) \geq H(s) + H(s') + H(s'')$?

Fourthly, we would expect the same bounds for $b_{\Gamma''}$ as for $b_{\Gamma'}$ and so we could extend the construction in Section 7, Example 13 by having an extra $k-1$ imaginary participants in schemes σ and σ', and having a third scheme σ'', a geometric $(n, 2n-1)$ threshold scheme.

Another interesting generalisation is to consider threshold schemes that are not share-minimal. In such schemes it is possible to reduce the broadcast size at the expense of an increase in the amount of information stored as shares. As mentioned in Section 1, the extreme case of this concession is to give participants one share for every possible new threshold parameter set and then simply broadcast a message indicating which new set of shares to move to in order to enable the new parameter change. The pattern of the intermediate tradeoffs between this extreme case and the share-minimal schemes discussed in this paper remains undetermined and would be worthy of further investigation.

References

[1] S.G. Barwick, W.-A. Jackson, K.M. Martin and C.M. O'Keefe. *Optimal updating of ideal threshold schemes*, Preprint.

[2] S.G. Barwick, W.-A. Jackson, K.M. Martin and P.R. Wild. Size of broadcast in threshold schemes with disenrollment. *Information Security and Privacy, Lecture Notes in Comput. Sci.,* 2384, (2002), 71–88.

[3] G.R. Blakley, Safeguarding cryptographic keys, *Proceedings of AFIPS 1979 National Computer Conference*, 48, (1979), 313–317.

[4] B. Blakley, G.R. Blakley, A. Chan and J. Massey. Threshold schemes with disenrollment. *Adv. in Cryptology - CRYPTO'92, Lecture Notes in Comput. Sci.,* 740, (1993), 540–548.

[5] C. Blundo, A. Cresti, A. De Santis and U. Vaccaro. Fully dynamic secret sharing schemes. *Adv. in Cryptology - CRYPTO'93, Lecture Notes in Comput. Sci.,* 773, (1994), 110–125.

[6] C. Blundo, A. De Santis, G. Di Crescenzo, A. Giorgio Gaggia and U. Vaccaro. Multi-secret sharing schemes. *Adv. in Cryptology - CRYPTO'94, Lecture Notes in Comput. Sci.,* 839, (1994), 150–163.

[7] L. Chen, D. Gollmann and C.J. Mitchell. Key escrow in mutually mistrusting domains. *Security Protocols, Lecture Notes in Comput. Sci.,* 1189, (1997), 139–153.

[8] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, John Wiley & Sons, 1991.

[9] Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. *Preprint*, (1997).

[10] A. Herzberg, S. Jarecki, H. Krawczyk and M. Yung. Proactive secret sharing or: how to cope with perpetual leakage. *Adv. in Cryptology - CRYPTO'95, Lecture Notes in Comput. Sci.,* 963, (1995), 339–352.

[11] J.W.P. Hirschfeld. *Projective geometries over finite fields*, Clarendon Press, Oxford (1979).

[12] W.-A. Jackson and K.M. Martin. Perfect Secret Sharing Schemes on Five Participants, *Des., Codes, Cryptogr.* 9 (1996), 267–286.

[13] E. Karnin, J. Greene and M. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory* Vol. IT-29 (1983), 35–41.

[14] K.M. Martin. Untrustworthy participants in secret sharing schemes. *Cryptography and Coding III*, Oxford University Press, Oxford (1993), 255–264.

[15] K.M. Martin, R. Safavi-Naini and H. Wang. Bounds and techniques for efficient redistribution of secret shares to new access structures. *The Computer Journal*, Vol.42, No.8 (1999), 638–649.

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

[17] G.J. Simmons. Prepositioned shared secret and/or shared control schemes. *Adv. in Cryptology - EUROCRYPT'89, Lecture Notes in Comput. Sci.,* 434, (1990), 436–467.

[18] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their applications. *Contemporary Cryptology,* IEEE Press (1992), 441–497.

[19] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* 2 (1992), 357–390.

A Appendix: Information Theory

We provide a short introduction to entropy here, but refer the reader to, for example, [8] for details.

Let X be a finite set and let $\langle X\rangle$ be a finite collection of tuples, such that the entries of a tuple $\pi \in \langle X\rangle$ are indexed by the elements of X. Let ρ be a probability distribution on $\langle X\rangle$. For $\pi = (\pi_x)_{x\in X} \in \langle X\rangle$ and $A \subseteq X$, let $\pi_A = (\pi_x)_{x\in A}$ and let $\langle A\rangle = \{\pi_A | \pi \in X\}$. Let ρ_A be the marginal distribution on A, that is, ρ_A is the probability distribution on $\langle A\rangle$ such that for $\alpha \in \langle A\rangle$ we have $\rho_A(\alpha) = \sum_{\{\pi\in\langle X\rangle|\pi_A=\alpha\}} \rho(\pi)$. Let $[A]_\rho = \{\alpha \in \langle A\rangle \mid \rho_A(\alpha) > 0\}$. We use the notation (ρ, X) to denote the set of tuples $[X]_\rho$ indexed by X with the associated probability distribution ρ.

The *entropy* $H_\rho(A)$ of ρ_A is defined to be $H_\rho(A) = -\sum\limits_{\alpha\in[A]_\rho} \rho_A(\alpha)\log\rho_A(\alpha)$. We remark that the base of the logarithm is not specified here, but can be chosen to be any convenient value. Where there is no ambiguity, we will write $[A]$ for $[A]_\rho$ and H for H_ρ. Let $B \subseteq X$ and let $\beta \in [B]$. For $\alpha \in [A]$, we have the conditional probability

$$\rho_{A|B}(\alpha, \beta) = \frac{\sum_{\{\pi\in\langle X\rangle|\pi_A=\alpha,\pi_B=\beta\}} \rho(\pi)}{\rho_B(\beta)}.$$

We may write $\rho_{A|B=\beta}$ for $\rho_{A|B}(\alpha, \beta)$, so we can regard $\rho_{A|B=\beta}$ as a probability distribution on $[A]_\rho$. The *conditional entropy* $H(A|B = \beta)$ of $\rho_{A|B=\beta}$ is defined to be

$$H(A|B = \beta) = -\sum_{\alpha\in[A]} \rho_{A|B}(\alpha, \beta)\log\rho_{A|B}(\alpha, \beta).$$

The *conditional entropy* $H(A|B)$ of ρ_A given ρ_B is defined to be

$$H(A|B) = \sum_{\beta\in[B]} H(A|B = \beta)\rho_B(\beta)$$

and it can be shown that $H(A|B) = H(AB) - H(B)$. Note that if $H(A|B) = H(A)$ then A and B are independent variables and so $\rho_{A|B}(\alpha, \beta) = \rho_A(\alpha)$. Hence $H(A|B) = H(A)$ implies that $H(A|B = \beta) = H(A)$.

For $C \subseteq X$, the *mutual information* $I(A; B \mid C)$ of ρ_A and ρ_B given ρ_C is defined to be

$$I(A; B \mid C) = H(A|C) - H(A|BC).$$

If $C = \emptyset$, we write $I(A; B)$ for $I(A; B \mid \emptyset)$. The following inequalities can be shown:

$$I(A; B \mid C) \geq 0,$$

$$H(A) \geq H(A|B) \geq 0.$$

B Appendix: Proofs and Technical Results

B.1 Preliminary Results for Dynamic Threshold Schemes

We first prove three lemmas that we will need later. The first lemma notes that for a large class of regions $\mathcal{U}$ the secrets s and s' must be independent.

Lemma 14 *If there exists $\Gamma' \in \mathcal{U}$ with $\Gamma \not\subseteq \Gamma'$, then $H(s' \mid s) = H(s')$.*

Proof: Suppose $\Gamma \not\subseteq \Gamma'$, so there exists a set $A \subseteq \mathcal{P}$ with $A \in \Gamma$ but $A \notin \Gamma'$. Suppose $H(s'|s) < H(s')$. As $H(s|A) = 0$, we have $H(s'|Ab_{\Gamma'}) = H(s'|Ab_{\Gamma'}s) \leq H(s'|s) < H(s')$, contradicting (B) in Definition 6. Hence $H(s'|s) = H(s')$. □

The next observation is an adaptation of a result in [6].

Lemma 15 *If there exists $\Gamma' \in \mathcal{U}$, $p \in \mathcal{P}$ and sets $X, X' \subseteq \mathcal{P}$ with $X \notin \Gamma$, $pX \in \Gamma$, $XX' \in \Gamma$, $XX' \notin \Gamma'$, $pXX' \in \Gamma'$, then $H(p) \geq H(s) + H(s')$.*

Proof: Using the relationships in Section A,

$$\begin{array}{rcll}
H(p) & \geq & H(p \,|\, X) & \\
& = & H(s \,|\, X) - H(s \,|\, pX) + H(p \,|\, sX) & \\
& = & H(s) + H(p \,|\, sX) & \text{as } X \notin \Gamma \text{ and } pX \in \Gamma \\
& \geq & H(s) + H(p \,|\, sXX'b_{\Gamma'}) & \\
& = & H(s) + H(s' \,|\, sXX'b_{\Gamma'}) - H(s' \,|\, psXX'b_{\Gamma'}) + H(p \,|\, ss'XX'b_{\Gamma'}) & \\
& = & H(s) + H(s' \,|\, sXX'b_{\Gamma'}) + H(p \,|\, ss'XX'b_{\Gamma'}) & \text{as } pXX' \in \Gamma' \\
& = & H(s) + H(s') + H(p \,|\, ss'XX'b_{\Gamma'}) & \text{as } XX' \in \Gamma \text{ and } XX' \notin \Gamma' \\
& \geq & H(s) + H(s'). &
\end{array}$$

□

Lemma 16 *Consider any probability distribution on a set $\langle Z \rangle$ with $s', p \in Z$, $X \subseteq Z$. Suppose s', X and p satisfy $s' \notin X$, $p \notin Xs'$, $H(s' \,|\, X) = H(s')$ and $H(s' \,|\, Xp) = 0$. Then $H(p \,|\, X) \geq H(s')$.*

Proof: $H(p \,|\, X) = H(pX) - H(X) = H(s'pX) - H(s'X) + H(s') = H(p \,|\, s'X) + H(s') \geq H(s')$. □

B.2 Proofs for Section 4

This sections contains the proofs for Theorems 7 and 8 of Section 4.

B.2.1 Proof of Theorem 7

Proof: Let Γ' be the (n,n)-threshold structure on $\mathcal{P}$, so $\Gamma' \in \mathcal{U}^+$.

(a) Let $A \subseteq \mathcal{P}$ be such that $|A| = k$. Since $k < n$, $A \in \Gamma \setminus \Gamma'$. By Lemma 14, $H(s' \,|\, s) = H(s')$.

(b) For $p \in \mathcal{P}$, let $X \subseteq \mathcal{P} \setminus p$ be a set of size $k-1$ and $X' = \mathcal{P} \setminus (pX)$. Applying Lemma 15 and (1) we get $H(p) \geq H(s) + H(s') = 2H(s)$. □

B.2.2 Proof of Theorem 8

We proceed to prove this result by induction, commencing with the case $k = 1$ and then the general case.

Increasing the threshold: the case $\mathbf{k = 1}$

We aim to prove the lower bound on the broadcast size for the case $k = 1$. We first prove two technical lemmas and then establish the bound for this case.

Let $n > 1$ and $\mathcal{M} = (\rho, ss'\mathcal{P}\mathcal{B})$ be a share minimal $(1, n)$-threshold scheme that can be updated to $\mathcal{U}^+(1, n)$. Let $\Gamma' \in \mathcal{U}^+(1, n)$ be a (k', n')-threshold structure on $\mathcal{P}' \subseteq \mathcal{P}$. By share minimality we have $H(p) = 2H(s)$ for each $p \in \mathcal{P}$. Essentially, one part of each share can be thought of as relating to the original $(1, n)$-threshold structure Γ and the other part can be thought of as relating to the new threshold structure $\Gamma' \in \mathcal{U}^+(1, n)$. To see this, we factor out the first part by letting $\sigma \in [s]$ and defining a new probability distribution τ on $\langle s'\mathcal{P}\mathcal{B}\rangle_\rho$ by $\tau = \rho_{s'\mathcal{P}\mathcal{B}|s=\sigma}$. The following lemma shows that $(\tau, s'\mathcal{P}\mathcal{B})$ is "almost" a (k', n')-threshold scheme.

Lemma 17 *Let $\sigma \in [s]$ and $A \subseteq \mathcal{P}'$ be a k'-set. Then*

(a) $H_\tau(s') = H(s')$;

(b) $H_\tau(p) = H_\tau(s')$;

(c) $H_\tau(s' \mid Ab_{\Gamma'}) = 0$;

(d) $H_\tau(s' \mid (A \setminus p)(\mathcal{P} \setminus \mathcal{P}')b_{\Gamma'}) = H_\tau(s')$ *for any* $p \in A$.

Proof: By definition we have

$$\begin{aligned} H(s' \mid Ab_{\Gamma'}) &= 0 && (2) \\ H(s' \mid (A \setminus p)b_{\Gamma'}(\mathcal{P} \setminus \mathcal{P}')) &= H(s') \quad \text{for all } p \in A. && (3) \end{aligned}$$

Part (a) follows immediately by noting that Theorem 7 (a) implies that $\rho_{s'} = \tau_{s'}$. Now choose $X \subseteq \mathcal{P}$, $X \neq \emptyset$. It follows from the definition of conditional entropy that

$$\sum_{\sigma \in [s]} \rho_s(\sigma) H_\tau(s' \mid b_{\Gamma'} X) = H(s' \mid b_{\Gamma'} X s) = H(s' \mid b_{\Gamma'} X) \qquad (4)$$

as $|X| \geq 1$ implies $H(s|X) = 0$.

To prove part (c), let $X = A$. By (2) and (4) it follows that $H_\tau(s' \mid b_{\Gamma'} A) = 0$, as required. For part (d), let $p \in A$ and choose $X = (A \setminus p)(\mathcal{P} \setminus \mathcal{P}')$. Since $H_\tau(s' \mid b_{\Gamma'} X) \leq H_\tau(s')$ for all $\sigma \in [s]$, by (3) and (4) it follows that $H_\tau(s' \mid b_{\Gamma'} X) = H_\tau(s')$, as required.

Finally for part (b), apply Lemma 16 to (c) and (d) to obtain $H_\tau(p) \geq H_\tau(s) = H(s')$, the equality by (a). As $\sum_{\sigma \in [s]} \rho_s(\sigma) H_\tau(p) = H(p \mid s) = H(s \mid p) + H(p) - H(s) = H(p) - H(s) = H(s)$, it follows that $H_\tau(p) = H(s)$ for all $\sigma \in [s]$. □

We now prove some further properties of τ before establishing the bound.

Lemma 18 *With respect to τ:*

(a) *The variables* $\{p \mid p \in \mathcal{P}\}$ *are independent.*

(b) *For* $p \in \mathcal{P}$*, we have* $H_\tau(s' \mid (\mathcal{P} \setminus p)) = H_\tau(s')$.

(c) *If* $Y \subseteq \mathcal{P}'$ *is a* $(k'-1)$*-set then* $H_\tau(p \mid b_{\Gamma'} Y s') = 0$.

Proof: (a) To show independence, we show that $H_\tau(p \mid (\mathcal{P} \setminus p)) = H_\tau(p)$. Let $\Gamma' \in \mathcal{U}^+(1,n)$ be the $(1,1)$-threshold structure on $\mathcal{P}' = \{p\}$. From Lemma 17(c) and (d) we have $H_\tau(s' \mid \mathcal{P} b_{\Gamma'}) = 0$ and $H_\tau(s' \mid (\mathcal{P} \setminus p) b_{\Gamma'}) = H_\tau(s')$. Applying Lemma 16 we get $H_\tau(s') \leq H_\tau(p \mid (\mathcal{P} \setminus p) b_{\Gamma'}) \leq H_\tau(p)$. The result follows by Lemma 17(b).

(b) Let $\Gamma' \in \mathcal{U}^+(1,n)$ be the (n,n)-threshold structure. Then, for $p \in \mathcal{P}$, $\mathcal{P} \setminus p \notin \Gamma'$. Thus by Lemma 17 (d), $H_\tau(s' \mid (\mathcal{P} \setminus p) b_{\Gamma'}) = H_\tau(s')$ and so $H_\tau(s' \mid (\mathcal{P} \setminus p)) = H_\tau(s')$.

(c) Using the results of Section A,

$$\begin{aligned}
0 &\leq H_\tau(p \mid b_{\Gamma'} Y s') \\
&= H_\tau(b_{\Gamma'} p Y s') - H_\tau(b_{\Gamma'} Y s') \\
&= H_\tau(b_{\Gamma'} p Y) - H_\tau(b_{\Gamma'} Y s') \quad \text{by Lemma 17(c)} \\
&= H_\tau(b_{\Gamma'} p Y) - H_\tau(b_{\Gamma'} Y) - H_\tau(s') \quad \text{by Lemma 17(d)} \\
&= H_\tau(p \mid b_{\Gamma'} Y) - H_\tau(s') \\
&\leq H_\tau(p) - H_\tau(s') \\
&= 0 \quad \text{by Lemma 17(b).}
\end{aligned}$$

Hence equality holds throughout. □

We can now prove the lower bound on the size of broadcast for the case $k = 1$.

Lemma 19 *Let* $\mathcal{M} = (\rho, ss'\mathcal{P}\mathcal{B})$ *be a share minimal* $(1,n)$*-threshold scheme with* $1 < n$ *that can be updated to* $\mathcal{U}^+(1,n)$*. Then for any* $\Gamma' \in \mathcal{U}^+(1,n)$ *where* Γ' *is a* (k',n')*-threshold structure,*

$$H(b_{\Gamma'}) \geq \begin{cases} (n'-k'+1)H(s) & \text{if } n' < n \\ (n'-k')H(s) & \text{if } n' = n. \end{cases}$$

Proof: Let $\Gamma' \in \mathcal{U}^+(1,n)$ be a (k',n')-threshold structure defined on $\mathcal{P}' = \{p_1, \ldots, p_{n'}\}$.

$$\begin{aligned}
H_\tau(b_{\Gamma'}) &= H_\tau(b_{\Gamma'} \mid s') + \mathrm{I}_\tau(b_{\Gamma'}; s') \\
&= H_\tau(b_{\Gamma'} \mid s') \quad \text{as } \mathrm{I}_\tau(b_{\Gamma'}; s') = 0 \text{ by (3)} \\
&= H_\tau(b_{\Gamma'} \mid p_1, \ldots, p_{n'} s') + \mathrm{I}_\tau(b_{\Gamma'}; p_1, \ldots, p_{n'} \mid s') \\
&\geq \mathrm{I}_\tau(b_{\Gamma'}; p_1, \ldots, p_{n'} \mid s') \\
&= H_\tau(p_1, \ldots, p_{n'} \mid s') - H_\tau(p_1, \ldots, p_{n'} \mid b_{\Gamma'} s') \\
&= H_\tau(p_1, \ldots, p_{n'} \mid s') - \sum_{i=1}^{n'} H_\tau(p_i \mid b_{\Gamma'} p_1, \ldots, p_{(i-1)} s')
\end{aligned}$$

For $1 \leq i \leq k'-1$ we have $H_\tau(p_i \mid b_{\Gamma'} p_1, \ldots, p_{(i-1)} s') \leq H_\tau(p_i) = H_\tau(s')$ by Lemma 17(b). For $k' \leq i \leq n'$ we have $H_\tau(p_i \mid b_{\Gamma'} p_1, \ldots, p_{(i-1)} s') = 0$ by Lemma 18(c). So

$$H_\tau(b_{\Gamma'}) \geq H_\tau(p_1, \ldots, p_{n'} \mid s') - (k'-1)H_\tau(s') \tag{5}$$

If $n' = n$, then by Lemma 18(a) the p_i are independent, and so

$$H_\tau(p_1, \ldots, p_{n'} \mid s') \geq (n'-1)H_\tau(s').$$

If $n' < n$, then by Lemma 18 we have

$$H_\tau(p_1, \ldots, p_{n'} \mid s') \geq n'H_\tau(s')$$

Combining the cases and using Lemma 17(a) and (1) we get

$$H_\tau(b_{\Gamma'}) \geq \begin{cases} (n'-k'+1)H(s) & \text{if } \ n' < n \\ (n'-k')H(s) & \text{if } \ n' = n. \end{cases}$$

As $H(b_{\Gamma'}) = \sum_{\sigma \in [s]} H_\tau(b_{\Gamma'})$, the theorem follows, as required. □

Increasing the threshold: the general case

We are now ready to prove Theorem 8 by induction on k.

If $k = 1$ then the result is proved by Lemma 19. Suppose $k > 1$. Let $K \subseteq \mathcal{P}$ be a $(k-1)$-set and let $\mathcal{Q} = \mathcal{P} \setminus K$. Let $\kappa \in [K]_\rho$ and let the probability distribution μ on $\langle ss'\mathcal{QB}\rangle_\rho$ be defined by $\mu = \rho_{ss'\mathcal{QB}|K=\kappa}$. As $\rho_K(\kappa) > 0$, it follows that $[ss'\mathcal{QB}]_\mu \neq \emptyset$.

Let $\mathcal{N} = (\mu, ss'\mathcal{QB})$ be the scheme corresponding to μ. In order to apply Lemma 19, we now show that $\mathcal{N}$ is a $(1, n-(k-1))$-threshold scheme that can be updated to $\mathcal{U}^+(1, n-(k-1))$, for an appropriate choice of broadcast.

Let $p \in \mathcal{Q}$. Now $H(s \mid pK) = 0$ so $0 = H(s \mid p(K = \kappa)) = H_\mu(s \mid p)$, as required. Since $|K| < k$, $H(s \mid K = \kappa) = H(s)$ and so $H_\mu(s) = H(s)$. Part (A) of Definition 6 is thus satisfied.

Let $\Pi \in \mathcal{U}^+(1, n-(k-1))$ be an (l,m)-threshold access structure on $\mathcal{Q}' \subseteq \mathcal{Q}$. Let Γ' be the (k', n')-threshold structure on $\mathcal{P}' = K\mathcal{Q}'$ with $k' = l + (k-1)$ and $n' = m + (k-1)$. We show that $b_{\Gamma'}$ is the broadcast variable for Π in μ. Let $A \subseteq \mathcal{Q}'$ be a l-set, so $|AK| = k'$. Since $\mathcal{M}$ can be updated to Γ', $H(s' \mid AKb_{\Gamma'}) = 0$. This implies that $H(s' \mid A(K = \kappa)b_{\Gamma'}) = 0$ and so $H_\mu(s' \mid Ab_{\Gamma'}) = 0$. Now let $p \in A$. Since $H(s' \mid (A \setminus p)K(\mathcal{P} \setminus \mathcal{P}')b_{\Gamma'}) = H(s')$ it follows from Section A that $H_\mu(s' \mid (A \setminus p)(\mathcal{P} \setminus \mathcal{P}')b_{\Gamma'}) = H(s')$. Since $|K| < k'$, $H(s' \mid K) = H(s')$ and so $H_\mu(s') = H(s')$. Part (B) of Definition 6 is thus also satisfied.

So we have $\mathcal{N}$ a $(1, n-(k-1))$-threshold scheme which can be updated to $\Pi \in \mathcal{U}^+(1, n-(k-1))$ a (l,m)-threshold access structure using broadcast variable $b_{\Gamma'}$. We apply Lemma 19 to obtain

$$\begin{aligned} H_\mu(b_{\Gamma'}) \ &\geq \ \begin{cases} (m-l+1)H_\mu(s) & \text{if } \ m < n-(k-1) \\ (m-l)H_\mu(s) & \text{if } \ m = n-(k-1) \end{cases} \\ &= \ \begin{cases} (n'-k'+1)H_\mu(s) & \text{if } n' < n \\ (n'-k')H_\mu(s) & \text{if } n' = n \end{cases} \end{aligned}$$

Since we have already shown that $H(s) = H_\mu(s)$, and since

$$\begin{aligned} \sum_{\kappa \in [K]} \rho_K(\kappa) H_\mu(b_{\Gamma'}) \ &= \ \sum_{\kappa \in [K]} \rho_K(\kappa) H(b_{\Gamma'} \mid K = \kappa) \\ &= \ H(b_{\Gamma'} \mid K) \\ &\leq \ H(b_{\Gamma'}), \end{aligned}$$

and Theorem 8 is proved. □

Finally, we note that if the model is restricted to include the extra requirement that the participants belonging to Γ' cannot obtain s' prior to knowledge of the broadcast $b_{\Gamma'}$, (in other words $H_\tau(s' \mid \mathcal{P}) = H_\tau(s')$) then it follows that $H(p_1, \ldots, p_{n'} \mid s') = n'H(s)$ and from (5) we get the simplified bound of $H(b_{\Gamma'}) \geq (n'-k'+1)H(s)$, instead of the bound in Theorem 8.

B.3 Proofs for section 5

This section contains the proofs of Theorems 9 and 10 from Section 5.

B.3.1 Proof of Theorem 9

Proof: Let $\Gamma' \in \mathcal{U}_1^-$ be a $(1, n-k)$-threshold structure on $\mathcal{P}'$ (Γ' exists as $k < n$). Noting that $|\mathcal{P} \setminus \mathcal{P}'| = k$, choose $X \subseteq \mathcal{P} \setminus \mathcal{P}'$ to be a set of size $k-1$ and $X' \subseteq \mathcal{P} \setminus \mathcal{P}'$ to be a set of size 1 disjoint from X. Now let $p \in \mathcal{P}'$. The sets p, X, X' satisfy the conditions of Lemma 15, so we have $H(p) \geq H(s) + H(s') = 2H(s)$ by (1). □

B.3.2 Proof of Theorem 10

We have already seen that the two regions $\mathcal{U}_1^-$ and $\mathcal{U}_2^-$ are in some respects fundamentally different. In fact, to prove a lower bound on the broadcast size for updating to $\mathcal{U}^-$ we need two different approaches for each of these two regions. We prove these results separately in Theorems 21 and 22. The bound in Theorem 10 then follows immediately.

Decreasing the threshold: updating to $\mathcal{U}_1^-$

Recall that our aim is to establish a bound for updating to $\mathcal{U}^-$. In this section we consider schemes for updating to $\mathcal{U}^-$ but will only be concerned with how big the broadcast size is in the case that the new threshold parameters belong to $\mathcal{U}_1^-$. We proceed by induction on the new threshold parameter, first proving the bound for updating to $k' = 1$ and then for updating to general k'.

Lemma 20 *Let $\mathcal{M} = (\rho, ss'\mathcal{P}\mathcal{B})$ be a share minimal (k,n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^-$. Then for any $(1, n')$-threshold structure $\Gamma' \in \mathcal{U}_1^-$ defined on $\mathcal{P}' \subseteq \mathcal{P}$, $H(b_{\Gamma'}) \geq n'H(s')$.*

Proof: Let $\Gamma' \in \mathcal{U}_1^-$ be a $(1, n')$-threshold structure on $\mathcal{P}'$. Since $\Gamma' \in \mathcal{U}_1^-$ we have $n - n' > k - 1$. Let $X \subseteq \mathcal{P} \setminus \mathcal{P}'$ be a set of size $k-1$, let $X' \subseteq \mathcal{P} \setminus \mathcal{P}'$ be a set of size 1 disjoint from X and let $p \in \mathcal{P}'$.

As in the proof of Theorem 9, p, X and X' satisfy the conditions of Lemma 15. As $H(s) = H(s')$ and $H(p) = 2H(s)$, equality holds throughout the proof of Lemma 15. In particular,

$$\begin{aligned} H(p \mid sX) &= H(s') && (6) \\ H(p \mid sXX'b_{\Gamma'}) &= H(s') && (7) \\ H(s' \mid sXX'b_{\Gamma'}) &= H(s'). && (8) \end{aligned}$$

It follows from (8) that s and s' are independent.

For each $\omega \in [sX]$, define a new probability distribution τ on $\langle s'\mathcal{P}'\mathcal{B}\rangle_\rho$ by $\tau = \rho_{s'\mathcal{P}'\mathcal{B}|sX=\omega}$. From (8) it follows that $H(s' \mid sX) = H(s')$ and so

$$H_\tau(s') = H(s'). \tag{9}$$

Also by (8), $H(s' \,|\, sXb_{\Gamma'}) = H(s' \,|\, sX)$ and so $H_\tau(s' \,|\, b_{\Gamma'}) = H_\tau(s')$ (see Section A). Since $p \in \Gamma'$ we have $H(s' \,|\, psXb_{\Gamma'}) = 0$ and thus $H_\tau(s' \,|\, pb_{\Gamma'}) = 0$. By Lemma 16 it follows that $H_\tau(p \,|\, b_{\Gamma'}) \geq H_\tau(s')$ and hence $H_\tau(p) \geq H_\tau(s')$. By (6) and (9) it follows that

$$H_\tau(p) = H(s'). \tag{10}$$

Let $t \in \mathcal{P}$. Now consider updating to Δ, a $(1,1)$-threshold structure on $\mathcal{P}' = \{t\}$. So $\mathcal{P} \setminus t \notin \Delta$, that is $H(s' \,|\, (\mathcal{P} \setminus t)b_\Delta) = H(s')$ and $H(s' \,|\, \mathcal{P}\ b_\Delta) = 0$. So by Lemma 16, $H(t \,|\, (\mathcal{P} \setminus t)b_\Delta) \geq H(s')$. It follows that

$$H(t \,|\, \mathcal{P} \setminus t) \geq H(s') \text{ and } H(s' \,|\, \mathcal{P} \setminus t) = H(s'). \tag{11}$$

Returning to Γ', let $\mathcal{P}' = \{p_1, \ldots, p_{n'}\}$. Then $H_\tau(p_i \,|\, p_1, \ldots, p_{i-1}) \leq H_\tau(p_i) = H(s')$ by (10). Further, for $i \geq 2$,

$$\begin{aligned} H(p_i \,|\, p_1, \ldots, p_{i-1}sX) &= H(p_i \,|\, p_1, \ldots, p_{i-1}X) \quad \text{as } p_1X \in \Gamma \\ &\geq H(s') \quad \text{by (11)}. \end{aligned}$$

Hence $H_\tau(p_i \,|\, p_1, \ldots, p_{i-1}) = H(s')$ for $i \geq 2$. For $i = 1$, $H_\tau(p_1) = H(s')$ by (10). So

$$H_\tau(\mathcal{P}') = \sum_{i=1}^{n'} H_\tau(p_i \,|\, p_1, \ldots, p_{i-1}) = n'H(s'). \tag{12}$$

Since $(k-1) + n' < n$ and s, s' are independent, it follows from (11) that

$$H(s' \,|\, p_1, \ldots, p_{n'}sX) = H(s' \,|\, p_1, \ldots, p_{n'}X) = H(s'). \tag{13}$$

By (7), $H(p \,|\, sXb_{\Gamma'}) = H(s')$ and by (8), $H(s' \,|\, sXb_{\Gamma'}) = H(s')$. Now $H(p \,|\, s'sXb_{\Gamma'}) = H(s' \,|\, psXb_{\Gamma'}) + H(p \,|\, sXb_{\Gamma'}) - H(s' \,|\, sXb_{\Gamma'}) = 0 + H(s') - H(s') = 0$. Thus

$$H_\tau(p \,|\, b_{\Gamma'}s') = 0. \tag{14}$$

Thus,

$$\begin{aligned} H_\tau(b_{\Gamma'}) &\geq \mathrm{I}(b_{\Gamma'}; p_1 \ldots p_{n'} \,|\, s') \\ &= H_\tau(p_1 \ldots p_{n'} \,|\, s') - H_\tau(p_1 \ldots p_{n'} \,|\, b_{\Gamma'}s') \\ &= H_\tau(s' \,|\, p_1 \ldots p_{n'}) + H_\tau(p_1 \ldots p_{n'}) - H_\tau(s') - H_\tau(p_1 \ldots p_{n'} \,|\, b_{\Gamma'}s') \\ &= H_\tau(p_1 \ldots p_{n'}) - \sum_{i=1}^{n'} H_\tau(p_i \,|\, p_1 \ldots p_{i-1}b_{\Gamma'}s') \quad \text{by (9) and (13)} \\ &= n'H(s') \quad \text{by (12) and (14).} \end{aligned}$$

Thus we have $H(b_{\Gamma'}) = \sum_{\omega \in [sX]_\rho} \rho_{sX}(\omega) H_\tau(b_{\Gamma'}) \geq n'H(s')$, as required. $\square$

Theorem 21 *Let $\mathcal{M} = (\rho, ss'\mathcal{PB})$ be a share minimal (k,n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^-$. Then for any $\Gamma' \in \mathcal{U}_1^-$, where Γ' is a (k',n')-threshold structure, $H(b_{\Gamma'}) \geq (n' - k' + 1)H(s')$.*

Proof: The proof is similar to Theorem 8. If $k' = 1$ then the result is proved by Lemma 20. Suppose $k' > 1$ and Γ' is defined on $\mathcal{P}'$. Let $K \subseteq \mathcal{P}'$ be a $(k'-1)$–set and $\mathcal{Q}' = \mathcal{P}' \setminus K$. Let $\kappa \in [K]_\rho$ and let the probability distribution μ on $\langle ss'\mathcal{Q}'\mathcal{B}\rangle_\rho$ be defined by $\mu = \rho_{ss'\mathcal{Q}'\mathcal{B}|K=\kappa}$.

Let $\mathcal{N} = (\mu, ss'\mathcal{Q}'\mathcal{B})$ be the scheme corresponding to μ. In a similar way to the proof of Theorem 8 it can be shown that $\mathcal{N}$ is a $(k-(k'-1), n-(k'-1))$-threshold scheme which can be updated to $\Sigma' \in \mathcal{U}_1^-(1, n-(k'-1))$, with $H_\mu(s) = H_\mu(s') = H(s')$. It can be further shown that the broadcast for Σ' a $(1,m)$-threshold structure on $\mathcal{R}'$ is b_Σ, where Σ is the $(k', m+(k'-1))$-threshold structure on $\mathcal{R} = \mathcal{R}'K$. The broadcast corresponding to the $(1, n'-(k'-1))$-threshold structure on $\mathcal{Q}'$ is thus $b_{\Gamma'}$. By Lemma 20 we have

$$H_\mu(b_{\Gamma'}) \geq (n' - (k'-1))H_\mu(s).$$

However, by definition $H(b_{\Gamma'}) = \sum_{\kappa \in [K]} \rho_K(\kappa) H_\mu(b_{\Gamma'})$. Thus $H(b_{\Gamma'}) \geq (n' - k' + 1)H(s)$, as required. □

Decreasing the threshold: updating to $\mathcal{U}_2^-$

We now prove the complementary result to Theorem 21. Thus we consider schemes for updating to $\mathcal{U}^-$ but will only be concerned with how big the broadcast size is in the case that the new threshold parameters belong to $\mathcal{U}_2^-$.

Theorem 22 *Let $\mathcal{M} = (\rho, ss'\mathcal{P}\mathcal{B})$ be a share minimal (k,n)-threshold scheme with $k < n$ that can be updated to $\mathcal{U}^-$. Then, for any $\Gamma' \in \mathcal{U}_2^-$, where Γ' is a (k',n')-threshold structure, we have*

$$H(b_{\Gamma'}) \geq (\min(k,n') - k' + 1)H(s).$$

Proof: We divide the proof into three steps. In Step 1, we prove that for $A \subseteq \mathcal{P}$,

$$H(A) = (\min(k, |A|) + |A|)H(s). \tag{15}$$

In Step 2, for $\mathcal{M}$ as in the theorem and $\Gamma' \in \mathcal{U}_2^-(k,n)$ with Γ' a $(1,n')$-threshold structure (so $k - 1 \geq n - n'$), we will prove that

$$H(b_{\Gamma'}) \geq \min(k,n')H(s). \tag{16}$$

In Step 3 we complete the proof of the theorem.

We begin our proof. We note that since $\mathcal{M}$ can be updated to $\mathcal{U}^-$, equation (11) from the proof of Lemma 20 is valid. That is,

$$H(t \,|\, \mathcal{P} \setminus t) \geq H(s') \text{ and } H(s' \,|\, \mathcal{P} \setminus t) = H(s'). \tag{17}$$

Step 1. We first show that for any a–set A of $\mathcal{P}$, with $a \leq k$,

$$H(A) = 2aH(s). \tag{18}$$

We will do this by induction on k on the class of share minimal (k,n)-threshold schemes with $k < n$ which can be updated to $\mathcal{U}^-(k,n)$. If $k = 1$ then $H(p) = 2H(s)$ for $p \in \mathcal{P}$ as the scheme is share minimal. Our inductive hypothesis will be that (18) holds for all (ℓ, n)-threshold schemes with $1 \leq \ell \leq k$.

For a (k,n)-threshold scheme $(\rho, ss'\mathcal{P}\mathcal{B})$ with $1 < k < n$, let $p \in \mathcal{P}$ and let $\pi \in [p]_\rho$. Define ω on $\langle ss'(\mathcal{P} \setminus p)\mathcal{B}\rangle$ by $\omega = \rho_{ss'(\mathcal{P} \setminus p)\mathcal{B}|p=\pi}$.

It can be shown that $(\omega, ss'(\mathcal{P} \setminus p)\mathcal{B})$ is a share minimal $(k-1, n-1)$-threshold scheme with $1 \le k-1 \le n-1$, which can be updated to $\mathcal{U}^-(k-1, n-1)$. By inductive hypothesis, $H_\omega(A') = 2(a-1)H_\omega(s)$ for any set A' of $\mathcal{P} \setminus p$ of size $a-1$ $(1 \le a \le k)$. But $H_\omega(A') = H(A'|p = \pi)$, so $H(A'|p) = H_\omega(A') = 2(a-1)H(s)$. Hence $H(A'p) = H(A'|p) + H(p) = 2(a-1)H(s) + 2H(s) = 2aH(s)$, proving (18).

Now let X be a $(k-1)$–set, and let $p, q \in \mathcal{P} \setminus X$ with $p \neq q$. Thus $H(s|pX) = H(s|qX) = 0$ and $H(s|X) = H(s)$. However, we have $0 \le I(p; q|sX) = H(p|sX) - H(p|qsX) = H(psX) - H(sX) - H(p|qX)$ (as $H(s|qX) = 0$), which is equal to $H(s|pX) + H(pX) - H(s|X) - H(X) - H(p|qX) = 0 + 2kH(s) - H(s) - 2(k-1)H(s) - H(p|qX)$ by (18). Hence

$$H(p|qX) \le H(s). \tag{19}$$

We now prove (15). Let $A \subseteq \mathcal{P}$. If $|A| \le k$ then (15) holds by (18). So suppose $|A| = a > k$. Write $A = K \cup (A \setminus K)$ for a k–subset K of A. Let $A \setminus K = \{p_1, \ldots, p_{a-k}\}$. By (17) and (19)

$$H(s) \le H(p_i|p_1 \cdots p_{i-1}K) \le H(s)$$

for $1 \le i \le a-k$, and so

$$\begin{aligned} H(A) &= H(K) + \sum_{i=1}^{a-k} H(p_i|p_1 \cdots p_{i-1}K) \\ &= (2k + (a-k))H(s) \\ &= (k+a)H(s) \end{aligned}$$

proving (15) for the case $|A| = a > k$.

Step 2. Let $\mathcal{M}$ be as in the theorem and let $\Gamma' \in \mathcal{U}_2^-(k,n)$ be a $(1, n')$-threshold structure on $\mathcal{P}' \subseteq \mathcal{P}$, so $k-1 \ge n-n'$. Further,

$$\begin{aligned} H(s'|pb_{\Gamma'}) &= 0 \quad \text{for all } p \in \mathcal{P}' && (20) \\ H(s'|b_{\Gamma'}) &= H(s'). && (21) \end{aligned}$$

Now

$$\begin{aligned} H(p|b_{\Gamma'}s') &= H(s'|pb_{\Gamma'}) + H(pb_{\Gamma'}) - H(b_{\Gamma'}s') \\ &\le 0 + (H(p) + H(b_{\Gamma'})) - (H(b_{\Gamma'}) + H(s)) \quad \text{by (20) and (21)} \\ &= H(p) - H(s') = H(s'). \end{aligned} \tag{22}$$

If $n' = n$ let $Q = \mathcal{P}' \setminus p$ for some $p \in \mathcal{P}'$, otherwise $n' < n$ and let $Q = \mathcal{P}'$. Now

$$\begin{aligned} H(b_{\Gamma'}) \ge H(b_{\Gamma'}|s') &= H(b_{\Gamma'}|s'Q) + I(b_{\Gamma'}; Q|s') \\ &\ge I(b_{\Gamma'}; Q|s') \\ &= H(Q|s') - H(Q|b_{\Gamma'}s'). \end{aligned} \tag{23}$$

Now $H(Q|s') = H(Q)$ by (17), and by (15) we have $H(Q) = (\min(k, |Q|) + |Q|)H(s)$. Further, if $Q = \{p_1, \ldots, p_a\}$, then

$$H(Q|b_{\Gamma'}s') = \sum_{i=1}^{a} H(p_i|p_1 \cdots p_{i-1}b_{\Gamma'}s') \le \sum_{i=1}^{a} H(p_i|b_{\Gamma'}s') \le aH(s') \quad \text{by (22).} \tag{24}$$

Combining (23) and (24), $H(b_{\Gamma'}) \geq (\min(k,a) + a - a)H(s') = \min(k,a)H(s')$. Now if $n' < n$ then $a = n'$. Otherwise $n' = n$ and, as $k \leq n$, $\min(k,a) = k$. Thus $H(b_{\Gamma'}) \geq \min(k,n')H(s')$, proving (16).

Step 3. We now let $\Gamma' \in \mathcal{U}_2^-(k,n)$ be a (k',n')-threshold structure. If $k' = 1$ the result follows by (16). Suppose $k' > 1$. We proceed in a similar manner to the proof of Theorem 21. Let $K \subseteq \mathcal{P}'$ be a $(k'-1)$–set and let $\kappa \in [K]_\rho$. Let probability distribution μ on $\langle ss'(\mathcal{P} \setminus K)\mathcal{B}\rangle_\rho$ be defined by $\mu = \rho_{ss'(\mathcal{P} \setminus K)\mathcal{B}|K=\kappa}$. It can be shown that $\mathcal{N} = (\mu, ss'(\mathcal{P} \setminus K)\mathcal{B})$ is a share minimal $(k-(k'-1), n-(k'-1))$-threshold scheme which can be updated to $\mathcal{U}_2^-(k-(k'-1), n-(k'-1))$ with $H_\mu(s) = H_\mu(s') = H(s)$. For $\Sigma' \in \mathcal{U}_2^-(k-(k'-1), n-(k'-1))$, where Σ' is (l,m)-threshold on $\mathcal{Q}'$, the broadcast is $b_{\Sigma'}$ where Σ' is the $(l+(k'-1), m+(k'-1))$ access structure on $\mathcal{Q}'K$. Hence $b_{\Gamma'}$ is the broadcast in $\mathcal{N}$ for Π, where Π is the $(1, n'-(k'-1))$-threshold structure on $\mathcal{P}' \setminus K$. By (16) we have

$$H_\mu(b_{\Gamma'}) \geq \min(k-(k'-1), n'-(k'-1))H_\mu(s') \geq (\min(k,n') - k' + 1)H_\mu(s').$$

Now $H(b_{\Gamma'}) = \sum_{\kappa \in [K]} \rho_K(\kappa) H_\mu(b_{\Gamma'})$, so $H(b_{\Gamma'}) \geq (\min(k,n') - k' + 1)H(s')$, proving the theorem. $\square$

The bound in Theorem 10 now follows immediately from Theorems 21 and 22.