AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **36** (2006), Pages 123–132

Optimal updating of ideal threshold schemes

S.G. Barwick Wen-Ai Jackson*

Department of Pure Mathematics
University of Adelaide
SA 5005
Australia

Keith M. Martin

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

Christine M. O'Keefe

CSIRO Mathematical and Information Sciences
GPO Box 664, Canberra ACT 2601
Australia

Abstract

We consider the problem of changing the parameters of an established ideal (k, n)-threshold scheme without the use of secure channels. We identify the parameters (k', n') to which such a scheme can be updated by means of a broadcast message and then prove a lower bound on the size of the relevant broadcast. The tightness of this bound is demonstrated by describing an optimal procedure for updating the parameters of an ideal scheme.

1 Introduction

A (k, n)-threshold scheme [1, 2] 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 securely given by a trusted *dealer* to each participant on creation of the threshold scheme. An *ideal* (k, n)-threshold scheme [3] has the desirable properties that (i) knowledge of $k-1$ shares contributes no information to knowledge of the secret and

* This work was supported by the Australian Research Council.

(ii) each participant's share has minimal size (this is equal to the size of the secret). Most well-studied (k, n)-threshold schemes, such as the Shamir polynomial threshold schemes [2], are ideal.

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.

In this paper we are interested in the situation that occurs if the parameters of a (k, n)-threshold scheme need to change after the participants have received their initial shares. We refer to such a process as an *update*. Participants might need to be added or removed from the scheme (involving a change in n) or the security policy relating to the threshold scheme might need to be strengthened or slackened (involving a change in k), or indeed any combination of these changes. We make a number of assumptions about the method by which the update can take place. This clarifies the model in which we are working and distinguishes our approach from previous work:

1. *The only information held by a participant at the time of update is a share in an ideal (k, n)-threshold scheme.*
2. *The dealer no longer has access to secure channels in which to transfer private information to the participants.*
3. *Participants do not have access to any secure channels to communicate amongst themselves.*

The first assumption differentiates this approach from the techniques used in, for example, [4, 5, 6], where it is assumed that the dealer anticipates the need for future updates on initialisation of the threshold scheme and issues each participant with additional share information in order to facilitate them. The second assumption recognises the fact that there is a significant cost involved in the use of secure communications channels. This assumption rules out the "trivial" solution in which the dealer simply uses secure channels to issues "new" shares to all the participants involved in the new threshold scheme. The last assumption rules out *redistribution* techniques such as those discussed in [7].

As a result of the latter two assumptions, the only technique that the dealer can employ at the time of update is to use public channels to *broadcast* information that enables participants to determine shares in the new threshold scheme. Such broadcast information must be assumed to be readable by anyone, including non-participants in the threshold scheme. Although broadcasting is not as expensive a communication technique as using a secure channel, there are nonetheless environments where bandwidth is at a premium and minimising broadcasts is highly desirable.

In this paper we will first determine to which threshold parameters it is possible to update an ideal (k, n)-threshold scheme. We then establish the minimum size of the broadcast message necessary to conduct the update. Finally we provide an optimal update technique that uses this minimal broadcast.

2 Threshold schemes

We first present a summary of the background necessary for understanding the information theoretic model of a threshold scheme first proposed in [8]. This is the most natural model within which to prove bounds on information (in the particular case of this paper, broadcast) size. A more thorough introduction to entropy can be found in [9].

2.1 Information theory background

Let A and B be two finite sets. To simplify the set notation, we will denote $A \cup B$ by AB and simplify a single element set $\{x\}$ to x. Let X be a finite set and let $\langle X \rangle$ be a finite collection of tuples π that 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 $H_\rho(A) = -\sum_{\alpha \in [A]_\rho} \rho_A(\alpha) \log \rho_A(\alpha)$. 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 $\alpha \in [A]$, denote the conditional probability $A|B$ by

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

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 $H(A|B) = H(AB) - H(B)$. 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

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

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

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

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

2.2 Basic definition and examples

Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a set of participants, let s be the secret variable, and let k be an integer with $1 \leq k \leq n$. A (k, n)-*threshold scheme* $\mathcal{M} = (\mathcal{P}, s, \rho)$ 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 $A \subseteq \mathcal{P}$,

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

Note that threshold schemes defined as above are often referred to as being *perfect*. We call the elements of $[s\mathcal{P}]$ *distribution rules*. We call $H(p_i)$ the *size* of the share associated with p_i, and $H(s)$ the *size* of the secret. It can be seen (for example [10]) 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*.

In order to implement a threshold scheme, the collection $\Omega = [s\mathcal{P}]$ of distribution rules is made public. The dealer privately selects a distribution rule $\pi = (x_s, x_1, \ldots, x_n) \in \Omega$ 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. Ideal (k, n)-threshold schemes can be found for all integers $1 \leq k \leq n$ [1, 2]. We give two examples:

Shamir threshold schemes [2]. 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 $2 \leq k \leq n < p$. A dealer generates distinct, non-zero elements $x_1, \ldots, x_n$ of $\mathcal{Z}_p$ and publishes them. The dealer then secretly 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 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 obtain no information about the value of a_0, additional to the fact that it is in $\mathcal{Z}_p$. There are q^k distribution rules $(f(0), f(x_1), \ldots, f(x_n))$, corresponding to the q^k values of the k-tuple $(a_0, a_1, \ldots, a_{k-1})$. The probability distribution ρ is usually taken to be the uniform probability distribution (so each distribution rule is equally likely to occur).

Geometric schemes. An equivalent way to construct an ideal (k, n)-threshold scheme uses a geometric construction in $\Theta = \mathrm{PG}(k-1, q)$ (for a background in projective geometry see [11]). Let $\sigma : s\mathcal{P} \to \Theta$ 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. 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 [10].

3 Updating an ideal threshold scheme

We assume now that a dealer has distributed shares of an ideal (k, n)-threshold scheme $\mathcal{M} = (\mathcal{P}, s, \rho)$ to participants $\mathcal{P}$. We now investigate how to update $\mathcal{M}$ to a (k', n')-threshold scheme under the constraints described in Section 1.

The assumptions that there are no secure channels available immediately rule out the addition of new participants to the scheme since it is not possible for any new participant to obtain private information by this technique. For the rest of the paper we thus assume that $n' \leq n$ and that the resulting new threshold scheme is defined on a subset $\mathcal{P}' \subseteq \mathcal{P}$ of participants, with the secret in this new scheme being the same as that of the original.

A (k, n)-threshold scheme $\mathcal{M} = (\mathcal{P}, s, \rho)$ can be *updated to* (k', n') if for every n'-subset $\mathcal{P}' \subseteq \mathcal{P}$ there exists a *broadcast variable* b (taking values from a set $[b]$) and a probability distribution τ defined on a collection $\langle s\mathcal{P}b\rangle$ of tuples, each indexed by the elements of $s\mathcal{P}b$, such that:

(A) $\tau_{s\mathcal{P}} = \rho$.

(B) for each $\beta \in [b]$, $\mathcal{M}_\beta = (\mathcal{P}, s, \tau^\beta)$ is effectively an ideal (k', n')-threshold scheme on $\mathcal{P}'$ with $H_{\tau^\beta}(s) = H_\rho(s)$, where $\tau^\beta = \tau_{s\mathcal{P}|b=\beta}$; in other words, for each $A \subseteq \mathcal{P}$ we have

$$H_\tau(s \mid Ab) = \begin{cases} 0 & \text{if } |A \cap \mathcal{P}'| \geq k', \\ H_\tau(s) & \text{if } |A \cap \mathcal{P}'| < k'. \end{cases}$$

Property (A) says that for any $A \subseteq s\mathcal{P}$, $H_\rho(A) = H_\tau(A)$. Since τ is thus an extension of ρ from $\langle s\mathcal{P}\rangle$ to $\langle s\mathcal{P}b\rangle$, to simplify we will abuse notation (slightly!) and generally write H for both H_ρ and H_τ throughout the rest of the paper.

3.1 Parameters to which an ideal scheme can be updated

We now examine the parameters (k', n') to which it is possible to update an ideal (k, n)-threshold scheme.

Lemma 1 *Let $\mathcal{M} = (\mathcal{P}, s, \rho)$ be an ideal (k, n)-threshold scheme that can be updated to (k', n'). Let b be the broadcast variable associated with $\mathcal{P}'$. Then for each $p \in \mathcal{P}'$ and $\beta \in [b]$ we have $H_{\tau^\beta}(p) = H(p)$.*

Proof: Since $\mathcal{M}$ and $\mathcal{M}_\beta$ are both ideal, we have $H_{\tau^\beta}(p) = H_{\tau^\beta}(s) = H(s) = H(p)$. □

Theorem 2 *Let $\mathcal{M} = (\mathcal{P}, s, \rho)$ be an ideal (k, n)-threshold scheme that can be updated to (k', n'). Then $k - k' \geq n - n'$.*

Proof: Let b be the broadcast associated with $\mathcal{P}'$. Let $A \subseteq \mathcal{P}'$ be a $(k' - 1)$–set and let $X = \mathcal{P} \setminus \mathcal{P}'$. As $|AX \cap \mathcal{P}'| = k' - 1$, we have

$$H_{\tau^\beta}(s \mid AX) = H_{\tau^\beta}(s) > 0. \tag{1}$$

Suppose $H(s|AX) = 0$. So $0 = H(s \,|\, AXb) = \sum_{\beta \in [b]} \tau_b(\beta) H_{\tau^\beta}(s \,|\, AX)$. As $H_{\tau^\beta}(s \,|\, AX) \geq 0$, it follows that $H_{\tau^\beta}(s \,|\, AX) = 0$, contradicting (1). Thus $H(s \,|\, AX) > 0$, so $|AX| \leq k-1$. It follows that $(k'-1) + (n-n') \leq k-1$, and hence $k - k' \geq n - n'$. □

Note that an immediate consequence of Theorem 2 is that, since $n' \leq n$, we have $k' \leq k$. It is thus not possible to update an ideal (k,n)-threshold scheme to one with an increased threshold.

3.2 Determining the minimum broadcast

We now prove the main result of this paper by determining a lower bound on the size of broadcast message necessary to update an ideal (k,n)-threshold scheme. First we recall an important fact concerning ideal threshold schemes that has been proved in, for example, [3, 12].

Lemma 3 *Let $\mathcal{M} = (\mathcal{P}, s, \rho)$ be an ideal (k,n)-threshold scheme. Then for any $X \subseteq s\mathcal{P}$ such that $|X| \leq k-1$, the variables in X are independent.*

Theorem 4 *Let $\mathcal{M} = (\mathcal{P}, s, \rho)$ be an ideal (k,n)-threshold scheme that can be updated to (k', n'). Let b be the broadcast variable associated with $\mathcal{P}' \subseteq \mathcal{P}$. Then*

$$H(b) \geq \min(k-k', n'-k'+1) H(s).$$

Proof: By Theorem 2, $k - k' \geq n - n' \geq 0$. If $k = k'$ then $n' = n$ and so the result is trivial. We thus assume that $k' < k$.

We first prove the theorem in the case $k' = 1$. Let $p \in \mathcal{P}'$ and $\beta \in [b]$. As $k' = 1$, by definition we have

$$H(s \,|\, pb) = 0 \text{ and } H(s \,|\, b) = H(s). \tag{2}$$

Now

$$\begin{aligned} 0 \leq H(p \,|\, bs) &= H(pbs) - H(bs) \\ &= H(s \,|\, pb) + H(pb) - H(s \,|\, b) - H(b) \\ &= H(pb) - H(s) - H(b) \quad \text{by (2)} \\ &= H(p \,|\, b) - H(s) \\ &\leq H(p) - H(s) = 0. \end{aligned}$$

Thus equality holds throughout and so

$$H(p \,|\, bs) = 0 \quad \text{for all } p \in \mathcal{P}'. \tag{3}$$

However,

$$\begin{aligned} H(b) = H(b \,|\, s) + \mathrm{I}(b; s) &= H(b \,|\, s) + \mathrm{I}(s; b) \\ &= H(b \,|\, s) \quad \text{by (2)} \\ &= H(b \,|\, p_1 \ldots p_{k-1} s) + \mathrm{I}(b; p_1 \ldots p_{k-1} \,|\, s), \end{aligned}$$

where $p_1, \ldots, p_{k-1}$ are distinct elements of $\mathcal{P}'$ (if $n' \geq k-1$), or are the elements $p_1, \ldots, p_{n'}$ of $\mathcal{P}'$ plus $p_{n'+1}, \ldots, p_{k-1}$ from $\mathcal{P} \setminus \mathcal{P}'$ (if $n' < k-1$). Thus

$$\begin{aligned} H(b) \geq \mathrm{I}(b; p_1 \ldots p_{k-1} \,|\, s) &= \sum_{i=1}^{k-1} \mathrm{I}(b; p_i \,|\, p_1 \ldots p_{i-1} s) \\ &= \sum_{i=1}^{k-1} \left(H(p_i \,|\, p_1 \ldots p_{i-1} s) - H(p_i \,|\, p_1 \ldots p_{i-1} bs) \right) \\ &= (k-1)H(s) - \sum_{i=1}^{k-1} H(p_i \,|\, p_1 \ldots p_{i-1} bs) \quad \text{by Lemma 3.} \end{aligned}$$

Write $r_i = H(p_i \,|\, p_1 \ldots p_{i-1} bs)$ for $1 \leq i \leq k-1$. If $n' \geq k-1$ then $p_i \in \mathcal{P}'$ for all i, so by (3) we have $r_i = 0$ for all i, $1 \leq i \leq k-1$. Hence $H(b) \geq (k-1)H(s)$. If $n' < k-1$ then $r_i = 0$ for $1 \leq i \leq n'$ and $r_i \leq H(s)$ for $n' < i \leq k-1$. Hence $H(b) \geq (k-1)H(s) - (k-1-n')H(s) = n'H(s)$. Thus,

$$H(b) \geq \min(k-1, n')H(s), \tag{4}$$

proving the theorem for the case $k' = 1$.

Suppose now that $k' > 1$. Let $K \subseteq \mathcal{P}'$ be a $(k'-1)$–set. Let $\kappa \in [K]$ and $\mathcal{M}_\kappa = (\mathcal{P} \setminus K, s, \rho^\kappa)$, where $\rho^\kappa = \rho_{(s\mathcal{P} \setminus K)|K=\kappa}$. We show that $\mathcal{M}_\kappa$ is a $(k - (k'-1), n - (k'-1))$–threshold scheme that can be updated to $(1, n' - (k'-1))$.

Let $A \subseteq \mathcal{P} \setminus K$. By definition, $H(s \,|\, A(K = \kappa)) = 0$ if $|A| \geq k - (k'-1)$, and $H(s \,|\, A(K = \kappa)) = H(s)$ if $|A| < k - (k'-1)$. Thus $H_{\rho^\kappa}(s \,|\, A) = 0$ if $|A| \geq k - (k'-1)$, and $H_{\rho^\kappa}(s \,|\, A) = H_{\rho^\kappa}(s)$ if $|A| < k - (k'-1)$. So $\mathcal{M}_\kappa$ is indeed a $(k - (k'-1), n - (k'-1))$-threshold scheme.

Let b be the broadcast variable used to update $\mathcal{M}$ to $\mathcal{M}_\beta = (\mathcal{P}, s, \tau^\beta)$, effectively a (k', n')–threshold scheme on $\mathcal{P}'$, and τ be the associated probability distribution defined on $\langle s\mathcal{P}b \rangle$. Let $\tau^\kappa = \tau_{(s\mathcal{P}b \setminus K)|K=\kappa}$. Clearly $\tau^\kappa_{s\mathcal{P} \setminus K} = \rho^\kappa$, so (A) of the definition is satisfied.

Let $\beta \in [b]$ and $\tau^{\kappa\beta} = \tau^\kappa_{(s\mathcal{P} \setminus K)|b=\beta}$. We show that $\mathcal{M}_{\kappa\beta} = (\mathcal{P} \setminus K, s, \tau^{\kappa\beta})$ is effectively an ideal $(1, n' - (k'-1))$–threshold scheme on $\mathcal{P}' \setminus K$. Let $A \subseteq \mathcal{P} \setminus K$. First note that $H_{\tau^{\kappa\beta}}(s) = H_{\tau^\beta}(s \,|\, K = \kappa) = H_{\rho^\kappa}(s) = H(s)$, as $|K| < k'$. By definition of τ,

$$H_\tau(s \,|\, AKb) = \begin{cases} 0 & \text{if } |A \cap \mathcal{P}'| \geq 1 \\ H(s) & \text{if } |A \cap \mathcal{P}'| < 1. \end{cases}$$

So,

$$H_{\tau^\kappa}(s \,|\, Ab) = H_{\tau^\beta}(s \,|\, Ab(K = \kappa)) = \begin{cases} 0 & \text{if } |A \cap \mathcal{P}'| \geq 1 \\ H(s) & \text{if } |A \cap \mathcal{P}'| < 1 \end{cases},$$

satisfying part (B). Thus we have shown that $\mathcal{M}_\kappa$ is an ideal $(k-(k'-1), n-(k'-1))$-threshold scheme that can be updated to $(1, n' - (k'-1))$. Applying (4), we have

$$\begin{aligned} H_{\rho^\kappa}(b) &\geq \min(k - (k'-1) - 1, n' - (k'-1)) H_{\rho^\kappa}(s) \\ &= \min(k - k', n' - k' + 1) H(s). \end{aligned}$$

Since

$$H(b) \geq H(b \mid K) = \sum_{\kappa \in [K]} \rho_K(\kappa) H_{\rho^\kappa}(b),$$

the result follows. □

3.3 An optimal update technique

To show that the bound in Theorem 4 is tight, we give an example of an update technique based on an ideal geometric scheme (see Section 2.2) that attains the bound. Let $\Theta = \mathrm{PG}(k-1, q)$ and $\sigma\colon s\mathcal{P} \to \Theta$ be an ideal (k, n)-threshold scheme defined on $\mathcal{P} = \{p_1, \ldots, p_n\}$. Suppose we want to update σ to a (k', n')-threshold scheme defined on $\mathcal{P}' = \{p_1, \ldots, p_{n'}\}$, where $k - k' \geq n - n'$.

The dealer generates $t = (k - k') - (n - n')$ points $f_1, \ldots, f_t$ on the same normal rational curve as σ. These correspond to shares of t 'imaginary' participants. The dealer is able to generate these shares provided $q + 1 > n + t = k - k' + n'$ (as q is generally large compared to n, this is not restrictive). If the dealer broadcasts a message consisting of the shares $b = \{p^\sigma_{n'+1}, \ldots, p^\sigma_n, f_1, \ldots, f_t\}$ then the scheme effectively becomes a (k', n')-threshold scheme on $\mathcal{P}'$, since any k' participants in $\mathcal{P}'$ can pool their k' shares with the $n - n' + t = k - k'$ broadcast shares to obtain k shares, which can then be used to determine the secret s in the original (k, n)-threshold scheme. By a similar argument we can see that any $A \subseteq \mathcal{P}$ such that $|A \cap \mathcal{P}'| < k'$ learn nothing about s. This broadcast has size $H(b) = (k - k')H(s)$.

We can see from Theorem 4 that if $n' < k - 1$ then we should be able to do better than this, and indeed we can. Instead of broadcasting the $k - k'$ shares listed above, the dealer broadcasts the subspace $\Pi = \Sigma \cap \Sigma'$, where

$$\Sigma = \langle s^\sigma, p^\sigma_1, \ldots, p^\sigma_{n'} \rangle \quad \text{and} \quad \Sigma' = \langle p^\sigma_{n'+1}, \ldots, p^\sigma_n, f_1, \ldots, f_t \rangle.$$

Note that $\dim \Sigma = \min\{n', k-1\} = n'$ (as $n' < k-1$), $\dim \Sigma' = n - n' + t - 1 = k - k' - 1$ and $\langle \Sigma, \Sigma' \rangle = \Theta$. Thus $\Pi = \Sigma \cap \Sigma'$ has dimension $n' + (k - k' - 1) - (k - 1) = n' - k'$ and so $H(b) = n' - k' + 1$.

Note that Π contains none of $s^\sigma, p^\sigma_1, \ldots p^\sigma_{n'}$, as by definition Σ' cannot contain any further points of the normal rational curve. Suppose k' participants $X \subseteq \mathcal{P}'$ pool their shares. Note that $< X^\sigma, \Sigma' >= \Theta$ and so $X^\sigma \cap \Sigma' = \emptyset$. Thus $X^\sigma \cap \Pi = \emptyset$. So $\dim < X^\sigma, \Pi >= \dim X^\sigma + \dim \Pi - \dim X^\sigma \cap \Pi = (k' - 1) + (n' - k') - (-1) = n'$. As $< X^\sigma, \Pi > \subseteq \Sigma$ and $\dim \Sigma = n'$, it follows that $< X^\sigma, \Pi >= \Sigma$. That is, the shares in X together with the broadcast Π span Σ, which contains s, and so X can obtain the secret.

Now let $X \subseteq \mathcal{P}'$ be a set of size $k' - 1$ and let $Y = \langle X^\sigma, \Pi, p^\sigma_{n'+1}, \ldots, p^\sigma_n \rangle$. Let $Z = \langle X^\sigma, p^\sigma_{n'+1}, \ldots, p^\sigma_n, f_1, \ldots, f_t \rangle$. Clearly $Y \subseteq Z$, and Z is the span of $(k' - 1) + (n - n') + t = k - 1$ points of the normal rational curve. By the properties of the rational normal curve, $s^\sigma \notin Z$ and thus $s^\sigma \notin Y$. Hence the set $X \cup \{p_{n'+1}, \ldots, p_n\}$ cannot determine the secret s. Thus σ has been updated to (k', n').

Note that in the case $n' \geq k$ the two techniques result in the same broadcast, since $\dim \Sigma = k-1$, and so $\Sigma = \Theta$. Thus $\Pi = \Sigma \cap \Sigma' = \Sigma'$, which was the broadcast used in the first technique.

4 Closing remarks

We have considered the problem of updating the parameters of an ideal threshold scheme under the assumption that only broadcast messages can be used to conduct the parameter changes. We have established the minimum size of broadcast message necessary and exhibited an update technique for a family of ideal threshold schemes that has this minimal broadcast size. We make two closing remarks.

Firstly it would be nice to find an interpretation of the optimal construction exhibited in Section 3.3 for the more familiar Shamir ideal threshold schemes, based on polynomials. The Shamir ideal threshold schemes are easily interpreted as geometric schemes, but it is not always easy to sensibly reverse this interpretation and explain geometric properties in terms of polynomials. This problem remains open.

Secondly we observe that it is possible to update a (k, n)-threshold scheme to parameter sets other than those determined by Theorem 2 if the first assumption that the threshold scheme be ideal is dropped. In [4, 5, 6] schemes were designed explicitly with a future change of parameters in mind. Even if a change is not anticipated, by dropping the requirement that the scheme be ideal and permitting larger than necessary shares, it may be possible to exploit redundant information in the shares to enable a parameter update. This approach was attempted in [13], but we have not considered it further here as most threshold schemes that are not designed to have extended capabilities are implemented as ideal schemes.

References

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

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

[3] E.F. Brickell and D.M. Davenport. On the Classification of Ideal Secret Sharing Schemes, *J. Cryptology* **2** (1991), 123–134

[4] S.G. Barwick, W.-A. Jackson and K.M. Martin, Updating the parameters of a threshold scheme by minimal broadcast, *IEEE Trans. Info. Theory* **51** (2005), 620–633

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

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

[7] 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* **42** (1999), 638–649.

[8] E. Karnin, J. Greene and M. Hellman, On secret sharing systems, *IEEE Trans. Information Theory* **29** (1983), 35–41.

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

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

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

[12] W.-A. Jackson and K.M. Martin, Combinatorial models for perfect secret sharing schemes, *J. Combin. Math. Combin. Comput.* **28** (1998), 249–265.

[13] Y. Tamura, M. Tada and E. Okamoto, Update of access structure in Shamir's (k, n) threshold scheme, *Proc. 1999 Symposium on Cryptography and Information Security* **I** (1999), 469–474.

(Received 29 Apr 2005)