Open access • Book Chapter • DOI:10.1007/3-540-48970-3_15

Changing Thresholds in the Absence of Secure Channels — Source link

Keith M. Martin, Josef Pieprzyk, Reihaneh Safavi-Naini, Huaxiong Wang

Institutions: Katholieke Universiteit Leuven, University of Wollongong

Published on: 07 Apr 1999 - Australasian Conference on Information Security and Privacy

Topics: Shamir's Secret Sharing, Secure multi-party computation and Secret sharing

Changing Thresholds in the Absence of Secure Channels

Keith M. Martin*
Katholieke Universiteit Leuven
Dept. Elektrotechniek - ESAT
Kardinaal Mercierlaan 94
B-3001 Heverlee
Belgium
keith.martin@esat.kuleuven.ac.be

Josef Pieprzyk, Rei Safavi-Naini†and Huaxiong Wang
School of Information Technology and Computer Science
University of Wollongong
Northfields Avenue
Wollongong 2522
Australia

josef@cs.uow.edu.au
rei@cs.uow.edu.au
hw13@cs.uow.edu.au

Abstract

The ways the threshold parameter can be modified after the setup of a secret sharing scheme is the main theme of this work. The considerations are limited to the case when there are no secure channels. First we motivate the problem and discuss methods of threshold change when the dealer is still active and can use broadcasting to implement

*This work was supported by the European Commission under ACTS project AC095 (ASPeCT)

†This work was partially supported by the Australian Research Council under grant number A49703076

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

the change required. Next we study the case when participants themselves initiate the change of threshold without the dealer's help. A general model for threshold changeable secret sharing is developed and two constructions are given. The first generic construction allows the design of a threshold changeable secret sharing scheme which can be implemented using the Shamir approach. The second construction is geometrical in nature and is optimal in terms of the size of shares. The work is concluded by showing that any threshold scheme can be given some degree of threshold change capability.

1 Introduction

A (t, n)-*threshold scheme* is a method of splitting a secret piece of information among n participants in such a way that any t of the participants can together recover the secret. They do this by pooling together their *shares*, which are secret values securely transmitted to them by a *dealer* on initialisation of the threshold scheme. Threshold schemes [1, 15] are special examples of *secret sharing schemes*, which allow more general combinations of participants to collectively engage in recovery of the secret [17]. Secret sharing schemes, and in particular threshold schemes, have become an indispensable basic cryptographic tool in any security environment where active entities are groups rather than individuals [6]. The group of participants involved in a threshold scheme is not necessarily static over time. The number of participants and the threshold parameter may fluctuate reflecting the current structure of the organisation to whom the participants belong and the sensitivity of the secret. New participants may enter an organisation and need to be incorporated into the security structure (*enrolment*). Current participants may leave the organisation, their shares may become compromised, or their access to the secret may be withdrawn for security reasons (*disenrolment*). A high threshold parameter established on initialisation due to a high degree of mutual distrust among the participants may be relaxed as the participants mutual trust grows over time (*threshold decrease*). Alternatively mutual trust may decrease over time, perhaps due to organisational problems or security incidents, and hence the threshold parameters may require tightening (*threshold increase*). The longer the lifetime of a secret, the greater the chances that any of these alterations to the security policy in place on scheme initialisation are to occur, and hence the greater the likelihood that the threshold parameters may need to be changed. Such a need is related, but quite distinct, to the notion of *proac-*

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

tivity [10], where shares are refreshed at regular time intervals for security reasons, but where the threshold parameters do not change after each share refreshment. This motivates our interest in considering the problem of how to change the parameters of a (t, n)-threshold scheme after it has been initialised. In other words, how to obtain a (t', n')-threshold scheme from a (t, n)-threshold scheme. We assume that the secret is not reconstructed by the participants before the change of parameter. An obvious method of conducting such a change is for the dealer to issue new shares to all the participants in the new threshold scheme. This is an inefficient, and often impractical, solution as it involves the use of a secure communications from the dealer to each participant which may not be possible at the time the change of threshold is required. A possible method of enabling a change in the parameters of a threshold scheme is to conduct a secret *redistribution*. This technique was investigated for general secret sharing schemes in [7, 14]. A redistribution of the secret is conducted by the participants of the original scheme, and involves them communicating information among themselves, and among any new participants in the new scheme. Secret redistributions have two notable advantages in that they do not involve the dealer and that they can be conducted without any prior knowledge that a change of threshold parameters is required. However in general a redistribution requires the existence of secure communication links between the threshold scheme participants, which may be impossible or undesirable in many applications. In this paper we investigate how to change the parameters of a threshold scheme in the absence of either a secure link from the dealer to participants, or secure links between participants themselves. We restrict our attention to the cases of threshold increase and threshold decrease. Disenrolment in the absence of secure links has already been subject to investigation [2, 13]. It does not seem likely that enrolment is possible in the absence of any secure links (unless enrolling participants have already been issued with some advance information and have been operating as "sleeping" participants, which arguably does not count as fresh enrolment). In the following discussion we note that procedures for changing threshold can be classified by the amount of preparation for change that is made on the initialisation of the original threshold scheme. We will consider cases where the exact change of threshold parameter is known on initialisation, where only knowledge that a change (but not which change) is known on initialisation, and where no advance preparation for change is made. The new threshold will be agreed upon by sending messages over public channels. We distinguish two cases: the case that the original dealer is still active and the case that the original

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

dealer is no longer in existence and shareholders decide on the new threshold themselves. We assume that after such an agreement shareholders will behave honestly with respect to their agreed threshold and submit correct shares in reconstruction phase. A good example of a situation that change of threshold under the above conditions is required is when communication channels of t shareholders in a (t, n) threshold scheme are tapped by an enemy and hence an attempt to reconstruct the secret will enable the enemy to find the secret. By raising threshold to $t' > t$, the enemy will remain completely uncertain about the value of the secret. A second example is for distributing authority among a group of n participants and requiring two levels of collaboration, t and t', for two levels of security. This kind of multilevel security may also be seen as an option given to participants so that for more sensitive decisions a higher degree of agreement could be used. We also note that in some cases it may be desirable for the value of the secret to change when the threshold parameter changes. In general this is simply a matter of choice for threshold decrease. For threshold increase however, after the change of parameters certain sets that could previously access the secret may no longer be desired to. The paper is organised as follows. In Section 2, threshold schemes are introduced. Section 3 discusses general techniques for changing threshold by dealer broadcast. Section 4 introduces the model, derives bounds and proposes constructions for changing threshold without dealer assistance. Section 5 includes ideas on how an arbitrary threshold scheme can be made threshold changeable and Section 6 concludes the paper.

2 Threshold Schemes

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a group of n participants. Let S be the set of secrets and let the share of P_i come from set S_i. A (t, n)-threshold scheme is a pair of algorithms: the dealer and the combiner. For a given secret from S and some random string from $\mathcal{R}$, the dealer algorithm applies the mapping

$$\mathcal{D}_{t,n} : S \times R \rightarrow S_1 \times \ldots \times S_n$$

to assign shares to participants from $\mathcal{P}$. The shares of a subset $\mathcal{A} \subseteq \mathcal{P}$ of participants can be input into the combiner algorithm

$$\mathcal{C}_{t,n} : \bigcup_{P_i \in \mathcal{A}} \{S_i\} \rightarrow S,$$

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

which will return the secret if the set $\mathcal{A} \subseteq \mathcal{P}$ and $|\mathcal{A}| \geq t$, otherwise it fails. Each instance of the threshold scheme (pair (s, r), $s \in S$, $r \in R$) thus indexes a *distribution rule* and threshold scheme can be combinatorially represented by a matrix whose rows form the distribution rules, and columns are indexed by the secret and the participants. If we associate a probability with each $s \in S$ then a threshold scheme can also be described information theoretically using the entropy function [12]. More precisely, if $|\mathcal{A}| \geq t$ then $H(S|\mathcal{A}) = 0$, and if $|\mathcal{A}| < t$ then $H(S|\mathcal{A}) \neq 0$. A threshold scheme is *perfect* if $H(S|\mathcal{A}) = H(S)$ for any $|\mathcal{A}| < t$ (in other words groups of less than t participants learn no more information about the secret than is publicly known). Perfect threshold schemes with $H(S_i) = H(S)$ for all $i = 1, \ldots, n$ are said to be *ideal*. In general it can be assumed that in an ideal threshold scheme $S_i = S$ for each $i = 1, \ldots, n$. A consequence of the definition of a perfect threshold scheme is that the the size of shares is at least the size of the of the secret, that is $H(S_i) \geq H(S)$ [5]. If we reduce share size below that of the secret then it necessarily follows that the perfect property must be sacrificed. An example of threshold scheme that are not perfect are the so called *ramp schemes* [3, 9] which offer a compromise between security and share size. A (c, t, n)-ramp scheme is a (t, n)-threshold scheme such that:

1. If $\mathcal{A} \subseteq \mathcal{P}$ and $|\mathcal{A}| \geq t$, then $H(S|\mathcal{A}) = 0$;
2. If $\mathcal{A} \subseteq \mathcal{P}$ and $c < |\mathcal{A}| < t$, then $0 < H(S|\mathcal{A}) < H(S)$;
3. If $\mathcal{A} \subseteq \mathcal{P}$ and $|\mathcal{A}| \leq c$, then $H(S|\mathcal{A}) = H(S)$.

In [9] a (c, t, n)-ramp scheme with the property that $H(S_i) = H(S)/(t-c)$ for each $i = 1, \ldots, n$ is shown to be *optimal* (where an optimal ramp scheme is a ramp scheme where $H(S|A) = ((k-r)/(k-c))H(S)$ for $|A| = r, c \leq r \leq t$, and shares are of minimal size). Such schemes have nice properties and are easily constructed (see [9] for details).

3 Changing Threshold by Dealer Broadcast

In this section we assume that the original dealer of the threshold scheme is still active, but no longer able to use the secure links that were used to initiate the scheme. All messages from the dealer must thus take the form of broadcasts, where we assume that a broadcast message is an insecure communication that can be read by all participants and any outsiders to the scheme. There are two general techniques that can be used to change threshold by means of a broadcast message.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

1. *Advance key technique.* The dealer gives each participant a secret key as well as their share on initialisation. When the time comes to change threshold parameters, the dealer broadcasts new shares of the new threshold scheme, but encrypted under the secret keys issued to each participant. Unconditional security can be maintained by using a one-time pad to encrypt the information on this insecure channel.

2. *Advance share technique.* The dealer gives each participant shares in two different threshold schemes on initialisation. When the time comes to change threshold parameters, the dealer broadcasts specific shares of the second scheme that have the effect of changing the threshold parameters as required (see below).

The advance key technique would appear to be a somewhat trivial solution to the problem of changing thresholds by dealer broadcast. It does however suffer from the disadvantage that the size of the broadcast message is directly proportional to the number of participants in the scheme. The advance share technique can be used to reduce the broadcast size. A general example of the advanced share technique can be derived from techniques in [4, 13]. In this case, as well as their initial share in a (t, n)-scheme, on initialisation each participant is given a share in an $(n+1, 2n)$-scheme, which is defined on the n real participants, and n imaginary (*dummy*) participants. To realise a (t', n) scheme the dealer broadcasts $n - t' + 1$ shares of the $(n+1, 2n)$-scheme belonging to $n - t' + 1$ dummy participants. The resulting scheme is an $(n+1, 2n)$-scheme, contracted at $n - t' + 1$ participants: that is a $(t', n + t' - 1)$-scheme. However, $t' - 1$ of the shareholders are dummy participants and so the effective scheme is a (t', n)-scheme. The following comments apply to the two general techniques:

1. Both general techniques can be used when it is known on initialisation that a change of the threshold parameters may be needed, but not exactly what change will be necessary.

2. If the value of the secret changes when the threshold changes (i.e. the shares of the $(n+1, 2n)$-scheme correspond to a different secret than the original shares) then both threshold increase and decrease are possible using these techniques. If the value of the secret stays the same then in the case of threshold increase, participants must be trusted to move onto the new shares and not use their original ones (see comments in Section 1).

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

We can refine the advance share technique for threshold decrease if it is known on initialisation exactly what change in threshold parameter may be required. Let $t' < t$. . Let $m = \max(n, n') + (t - t')$. On initialisation, the dealer issues shares of a $(t, n + t - t')$-scheme to the n participants. The remaining $t - t'$ shares correspond to dummy participants and hence the resulting scheme is a (t, n)-scheme. To change this to a (t', n)-scheme the dealer broadcasts the $t - t'$ shares belonging to dummy participants. The resulting scheme is a $(t, n + t - t')$-scheme, contracted at $t - t'$ participants: that is, a (t', n)-scheme. The advantages of this refinement are that it is no longer necessary to issue an extra share in advance to each participant, and the broadcast message will usually be much shorter than for the general techniques.

4 Changing Threshold without Dealer Assistance

For the rest of this paper we assume that the dealer is no longer able to provide assistance in changing the threshold parameter. In the absence of both an active dealer and any secure channels between participants it is clear that participants can only use the information sent to them on initialisation of the original scheme. Hence the original "shares" must contain the information necessary for deriving both the shares of the initial (t, n)-scheme and the shares of the future (t', n)-scheme (we refer to these two derived shares as *subshares*). Such a system is therefore restricted in its application to situations where participants are trusted to operate "honestly" in the sense that during a reconstruction of the secret they only use the subshare that is relevant to the threshold in current use (see Section 1). A number of trivial solutions to this problem exist. If it is known in advance exactly what threshold change will be required then the initial share given to each participant could consist of one subshare corresponding to a share in the original (t, n)-scheme, and a second subshare that consists of a share in the later (t', n)-scheme. In this naive construction the required storage for each participant is $2H(S)$ (assuming the two systems are ideal). In general the size of the stored shares for each participant grows linearly with the number of required threshold which makes this method very inefficient. Another possible solution is to use the broadcast techniques of Section 2 and rely on a publicly accessible directory containing transcripts of the relevant broadcast messages for certain types of threshold change. Since participants are required to behave with a degree of honesty then they can be trusted to read

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

the relevant broadcast message at the appropriate time. These solutions do also generally involve more than one subshare being stored securely. We are thus interested in solutions that minimise the amount of information that each participant must store in order to derive both a (t, n) and (t', n)-scheme. The approach we will take is to construct (t, n)-schemes that can be changed into (t', n)-schemes through manipulation of the original shares. We will assume that $t' > t$ (threshold increase) and note that the schemes proposed could also be used for threshold decrease. For such schemes at least some advance knowledge of the future threshold change should be known on initialisation, since the schemes are designed to permit change. Later we consider some options for the much more difficult task of achieving some degree of change to an arbitrary threshold scheme (with no inbuilt mechanism in place to allow threshold change).

4.1 A Model for Threshold Change without Dealer Assistance

In this section we consider a basic model for schemes that permit threshold change without dealer assistance. We also discuss possible efficiency measures and then provide some constructions for such systems.

Definition 1 *A perfect (t, n)-threshold secret sharing with a dealer algorithm*

$$\mathcal{D}_{t,n} : S \times R \to S_1 \times \cdots \times S_n$$

is called threshold changeable to *t' if there exist publicly known functions $h_i : S_i \to T_i = h_i(S_i)$, for $1 \leq i \leq n$, such that $H(S|T_{\mathcal{A}}) = 0$ for any $|\mathcal{A}| \geq t'$, and $H(S|T_{\mathcal{A}}) < H(S)$ for any $|\mathcal{A}| < t'$ where $\mathcal{A} \subseteq \{1, \ldots, n\}$.*

¿From this definition, if we combine the dealer algorithm $\mathcal{D}_{t,n}$ with the functions h_i, we obtain the function

$$\mathcal{D}' : S \times R \to T_1 \times \cdots \times T_n$$

defined by $\mathcal{D}' = (h_1 \times \cdots \times h_n)\mathcal{D}_{t,n}$. It has the obvious properties

$$H(S|T_{\mathcal{A}}) = \begin{cases} 0 & \text{if } |\mathcal{A}| \geq t'; \\ H(S) & \text{if } |\mathcal{A}| < t, \end{cases}$$

for any $\mathcal{A} \subseteq \{1, \ldots, n\}$. Thus we may regard $\mathcal{D}'$ as a new dealer algorithm for a secret sharing scheme with n participants. In this model the subshare used

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

in the (t, n)-threshold scheme consists of the entire original share, and the subshare used in the (t', n)-threshold scheme is determined by the functions h_i.

4.2 Efficiency measures

We denote the (t, n)-threshold scheme by Π and the (t', n)-threshold scheme by Π'. The following lemma is fairly obvious.

Lemma 1 *Let Π be an ideal (t, n)-threshold scheme threshold changeable to $t' > t$. Then the resulting (t', n)-threshold scheme Π' is not perfect.*

Proof. By contradiction. Assume that the scheme Π' is ideal and perfect and any t' shares determine the secret. Thus $H(T_i) = H(S_i) = H(S)$. As the function h is deterministic we know that $H(T_i|S_i) = 0$. Since

$$I(S_i; T_i) = H(S_i) - H(S_i|T_i) = H(T_i) - H(T_i|S_i),$$

$H(T_i) = H(S_i)$ and $H(T_i|S_i) = 0$, then $H(S_i|T_i) = 0$. This means that there is a one-to-one correspondence between shares from Π and Π'. This also says that the threshold of Π' must be t' which gives us our requested contradiction. □

The efficiency of a perfect (t, n)-threshold scheme that is threshold changeable to t' can be measured by

1. the maximum and average size of the share which needs to be stored, given by $H(S_i)$, for $1 \leq i \leq n$,
2. the amount of information which needs to be delivered to the combiner at the pooling time expressed by $\sum_{i \in \mathcal{A}} H(T_i)$ for $\mathcal{A} \subseteq \{1, \ldots, n\}$ where $|\mathcal{A}| = t'$,
3. the size of subshares to be sent to the combiner, given by $H(T_i)$, for $1 \leq i \leq n$.

Theorem 2 *Let Π be a perfect (t, n)-threshold scheme that is threshold changeable to t' using functions $\mathcal{H} = \{h_i\}_{1 \leq i \leq n}$. Then*

1. *$H(S_i) \geq H(S)$ for $1 \leq i \leq n$;*
2. *$\sum_{i \in \mathcal{A}} H(T_i) \geq \frac{t'}{t'-t+1} H(S)$, for $\mathcal{A} \subseteq \{1, \ldots, n\}$ with $|\mathcal{A}| = t'$;*

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

3. $\max_{1\le i\le n}\{H(T_i)\} \ge \frac{1}{t'-t+1}H(S)$.

Proof. Part 1. follows by definition of perfect threshold scheme. We next prove part 3. Assume that $\mathcal{A}$ is a t' subset of $\{1,\ldots,n\}$ and $\mathcal{B}$ is a subset of $\mathcal{A}$ such that $|\mathcal{B}| = t-1$. We have

$$\begin{aligned} I(S;T_{(\mathcal{A}\setminus\mathcal{B})}|T_{\mathcal{B}}) &= H(S|T_{\mathcal{B}}) - H(S|T_{(\mathcal{A}\setminus\mathcal{B})},T_{\mathcal{B}}) \\ &= H(S|T_{\mathcal{B}}) - H(S|T_{\mathcal{A}}) \\ &= H(S|T_B) \\ &= H(S). \end{aligned}$$

On the other hand,

$$\begin{aligned} H(S;T_{(\mathcal{A}\setminus\mathcal{B})}|T_{\mathcal{B}}) &= H(T_{(\mathcal{A}\setminus\mathcal{B})}|T_{\mathcal{B}}) - H(T_{(\mathcal{A}\setminus\mathcal{B})}|T_{\mathcal{B}},S) \\ &\le H(T_{(\mathcal{A}\setminus\mathcal{B})} \\ &\le |\mathcal{A}\setminus\mathcal{B}|\max\{H(T_i;\ i\in\mathcal{A}\setminus\mathcal{B}\}) \\ &= (t'-t+1)\max\{H(T_i;\ i\in\mathcal{A}\setminus\mathcal{B}\}, \end{aligned}$$

proving part 3. To see part 2., let $\mathcal{A}$ be a t' subset of $\{1,\ldots,n\}$. For any subset $\mathcal{B}$ of $\mathcal{A}$ with $|\mathcal{B}| = t-1$, from proving part 2. we know that

$$\sum_{i\in\mathcal{A}\setminus\mathcal{B}} H(T_i) \ge H(S).$$

Let $\mathcal{F}$ be the collection of all $(t-1)$-subset of $\mathcal{A}$. We show that

$$\binom{t'-1}{t-1}\sum_{i\in\mathcal{A}} H(T_i) = \sum_{\mathcal{B}\in\mathcal{F}}\sum_{i\in\mathcal{A}\setminus\mathcal{B}} H(T_i).$$

Indeed, for each $i\in\mathcal{A}$, we denote $\mathcal{F}_i = \{\mathcal{B}\in\mathcal{F}; i\notin\mathcal{B}\}$. Then in the above equation $H(T_i)$ appears $|F_i| = \binom{t'-1}{t-1}$ times in the right-hand side for each $1\le i\le n$, and so the equation follows. We then have

$$\binom{t'-1}{t-1}\sum_{i\in\mathcal{A}} H(T_i) = \sum_{\mathcal{B}\in\mathcal{F}}\sum_{i\in\mathcal{A}\setminus\mathcal{B}} H(T_i) \ge \binom{t'}{t-1}H(S).$$

and obtain $\sum_{i\in\mathcal{A}} H(T_i) \ge \frac{t'}{t'-t+1}H(\mathcal{S})$. □

It is worth noting that item 2 shows that it is possible that the amount of information which needs to be delivered to the combiner at the pooling time is less than the original scheme ($tH(S)$) but of course the latter scheme is not perfect.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

Definition 2 *A perfect (t, n)-threshold scheme Π that is threshold changeable to t' is called* optimal *if the bounds in Theorem 2 are met with equality.*

Corollary 3 *If a perfect (t, n)-threshold scheme Π that is threshold changeable to t' is optimal then Π is ideal and Π' is a $(t-1, t', n)$ optimal ramp scheme.*

Proof. By definition Π is ideal and Π' is a $(t-1, t', n)$ ramp scheme. ¿From Theorem 2 (Part 2.) it follows that $H(T_i) = \frac{1}{t'-t+1}H(S)$ for all $1 \leq i \leq n$, and hence that the ramp scheme is optimal (see Section 2). □

4.3 A general construction from a ramp scheme

As noted earlier a naive (and very inefficient) method of allowing shareholders to choose among a number of thresholds is to give them independent subshares for each scheme. In this section we describe a much more efficient method of constructing a threshold scheme which can have a number of possible thresholds and has the property that original scheme is ideal. We give a general construction and then give the detail of an implementation based on Shamir polynomial scheme.

Theorem 4 *If there exists an optimal $((t-1)v, tv, nv)$-ramp scheme, then there exists a (t, n) threshold scheme that is threshold changeable to k for any integer k such that $k|vt$.*

Proof. Let Λ be an optimal $((t-1)v, tv, nv)$ ramp scheme. We can construct a (t, n) ideal threshold scheme Π from Λ as follows. As their initial share, give each participant in Π v different shares in Λ (we call these *component shares*. Since Λ is optimal, it is easy to verify that Π is a (t, n) ideal threshold scheme. We further define the conversion $\mathcal{H} = \{h_i\}_{1 \leq i \leq n}$ by letting the subshare of the (k, n)-scheme be formed by taking any vt/k component shares from the share of participant P_i (who has v component shares) for each $1 \leq i \leq n$. It is clear that k of these subshares will now be necessary to reconstruct the secret. □

Let u denote the number of integer k such that $k|vt$. The reduction in the size of storage for each shareholder compared to the naive method is $(u-1)H(S)$. A conceptually useful way of constructing ramp schemes suitable for use in Theorem 4 is to recall that by Theorem 9 [9], we know that if there exists a $(tv, nv + v - 1)$ ideal threshold scheme then there exists an optimal $((t-1)v, tv, nv)$ ramp scheme. A simple construction method is thus to

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

start with a Shamir threshold scheme [15], interpreted as a ramp scheme. Assume that $\mathcal{S} = GF(q)^v$ is the set of shares and secrets.

Construction

1. Let $q \geq nv$. To share a secret $s = (s_1, \ldots, s_v) \in GF(q)^v$ The dealer randomly chooses a polynomial $F(x)$ of degree at most $tv - 1$ such that $F(x)$ satisfies

   $$(F(1), \ldots, F(v)) = (s_1, \ldots, s_v).$$

   More precisely, $F(x)$ can be chosen in the following way. First select at random a vector $(s_{v+1}, \ldots, s_{tv}) \in GF(q)^{(t-1)v}$ and then use the Lagrange interpolation to compute the unique polynomial $F(x)$ of degree at most $tv-1$ satisfying $(F(1), \ldots, F(tv)) = (s_1, \ldots, s_{tv})$. Notice that the randomness of $(s_{v+1}, \ldots, s_{tv})$ results in the randomness of $F(x)$.

2. The dealer choose nv distinct numbers $x_1, \ldots, x_{nv}$ in $GF(q)\backslash\{1, \ldots, v\}$. Each participant P_i is assigned a subset $\mathcal{A}_i \subseteq \{x_1, \ldots, x_{nv}\}$ of v elements. $\mathcal{A}_i$ are public and unique for the participant P_i. Let $\mathcal{A}_i = \{x_{i_1}, \ldots, x_{i_v}\}$. The share of P_i is $S_i = F(\mathcal{A}_i) = (F(x_{i_1}), \ldots, F(x_{i_v}))$

3. At the pooling time, any t out of n participants can use the Lagrange interpolation to compute the polynomial $F(x)$ and so recover the secret $(F(1), \ldots, F(v))$.

The following comments apply to the above construction (and any other construction obtained using Theorem 4):

- Initially the scheme is clearly a (t, n)-threshold scheme. Any $t - 1$ participants have no information about which of the q^v candidates for the secret has been selected.
- Any k participants, each submitting (vt/k) parts of their share can reconstruct the secret.
- Any $k - 1$ participants A, each submitting (vt/k) parts of their share are left with $H(S|A) = (t/k)H(S)$, by definition of the ramp scheme.
- With respect to the bounds in Theorem 2, we have $H(S_i) = H(S)$, but $H(T_i) = (t/k)H(S)$. Thus such schemes will only be optimal in the degenerate case that $t = 1$.
- Each shareholder has $v \log q$ secret bits which is the same as the secret size.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

4.4 An optimal geometrical construction

The previous construction is conceptually simple and easy to implement. It is not however optimal. We now give an example of an optimal perfect (t, n)-threshold scheme that is threshold changeable to t'. This construction is described in terms of projective geometry, a technique first used for secret sharing schemes in [16]. For background information on projective geometry, see [11].

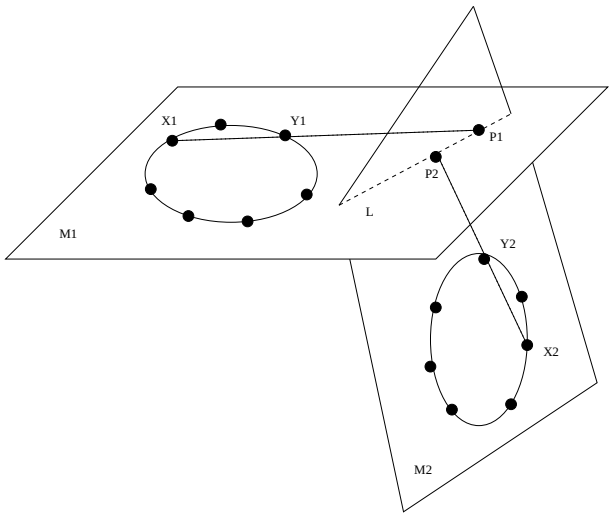

Figure 1: An optimal $(2, 7)$-scheme that is threshold changeable to 3

First note that $(1, 3, n)$-ramp scheme can be constructed in finite projective space as follows.

1. Let Π be a publicly known plane and let each line contained in Π represent a possible secret.
2. Pick another plane $\Pi 1$ that meets Π in a line $\mathcal{L}$.
3. Pick n points on $\Pi 1$, but not on $\mathcal{L}$, such that no three of the points are collinear. Give one point to each participant as their share of the secret.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

Any three shares consist of three non-collinear points, and thus knowledge of three shares is enough to generate the plane $\Pi 1$. Plane $\Pi 1$ can then be intersected with the public plane Π to recover the secret line $\mathcal{L}$. Any two shares $X1, Y1$ consist of two points which define a line $\langle X1, Y1 \rangle$. This line meets $\mathcal{L}$ in a unique point $P1$. Since it takes knowledge of two points on $\mathcal{L}$ to define $\mathcal{L}$, it follows that knowing two shares only reveals "half" of $\mathcal{L}$. Finally, any one share consists of one point not on $\mathcal{L}$, the span of which is naturally just that point and thus defines no points on $\mathcal{L}$. Hence knowledge of one share reveals nothing about the secret line $\mathcal{L}$. To see that such a configuration results in a set of mappings that fits the definition of ramp scheme in Section 2, see [8, 17]. Essentially there is one mapping for each plane $\Pi 1$ that meets plane Π in a line. Each secret line is represented by two points that generate that line. In each mapping, the share of a participant is one point, and the secret is two points, and hence $H(S_i) = H(S)/2$. In other words, the ramp scheme is optimal. We now extend this idea to construct an optimal perfect $(2, n)$-threshold scheme that is threshold changeable to 3.

1. Construct an optimal $(1, 3, n)$-ramp scheme on planes Π and $\Pi 1$ as before.

2. Pick another plane $\Pi 2$, distinct from Π and $\Pi 1$, that meets $\Pi 1$ (and Π) in line $\mathcal{L}$.

3. Construct an optimal $(1, 3, n)$-ramp scheme on plane $\Pi 2$. Each shareholder now holds a share that consists of two points, one on $\Pi 1$ and one on $\Pi 2$. The points of this second scheme must be allocated to shareholders in such a way that for any pair of shareholders, the unique point on $\mathcal{L}$ generated by their two points on $\Pi 1$ is distinct from the unique point on $\mathcal{L}$ defined by their two points on $\Pi 2$. Such an allocation of shares to shareholders is always possible (see closing remark in this section).

The resulting configuration is illustrated in Figure 1. Note that Π is not illustrated. In Figure 1 the share of participant X consists of points $X1$ and $X2$ (equivalently, line $\langle X1, X2 \rangle$), and the share of participant Y consists of points $Y1$ and $Y2$ (line $\langle Y1, Y2 \rangle$).

- Initially, shareholders use both their points to reconstruct the secret. Thus if shareholders X and Y try to reconstruct the secret then they can each use their point in each of the planes to generate the lines

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

$\langle X1, Y1\rangle$ and $\langle X2, Y2\rangle$, which meet Π in points $P1$ and $P2$ respectively. Since $P1$ and $P2$ are distinct, the two shareholders use these points to generate the secret $\mathcal{L}$. Further, each of the lines $\langle X1, X2\rangle$ and $\langle Y1, Y2\rangle$ are skew to $\mathcal{L}$ and hence one shareholder can not generate any points of $\mathcal{L}$. Thus the initial configuration can be used to generate a perfect $(2, n)$-threshold scheme.

- If shareholders just use their points on plane $\Pi 1$ then the result is the configuration of a $(1, 3, n)$-ramp scheme, as described previously. Hence any three participants can generate the secret, any two learn "one half" of the secret, and one shareholder learns nothing about the secret.

- The conversion of such a configuration into a scheme satisfying Definition 1 is identical to the conversion process described in [8, 17] for geometric secret sharing. The function h_i is simply the function that extracts the point on $\Pi 1$ from the pair of points allocated to the ith shareholder.

- The secret is represented by a line (two points). Each shareholder has a share consisting of two points. If the threshold is changed to three, then each shareholder only submits one point, exactly one half of their share. Thus with respect to the bounds in Theorem 2, we have $H(S_i) = H(S)$, and $H(T_i) = H(S)/2$. The scheme is thus optimal.

The above scheme generalises to a configuration for an optimal perfect (t, n)-threshold scheme that is threshold changeable to t' as follows:

1. Replace each plane Π by a space of projective dimension $t' - 1$.

2. Take $t' - t + 1$ of these spaces (instead of just two in Figure 1) such that all the spaces Πj meet in a subspace $\mathcal{L}$ of projective dimension $(t' - t)$.

3. On each space Πj choose n points such that no t' points lie together in a subspace of projective dimension $(t' - 2)$. This defines a $(t - 1, t', n)$-ramp scheme on Πj. When the threshold is increased to t', shareholders will submit only their points on space $\Pi 1$.

4. Any t points on any Π_j define a subspace of projective dimension $t - 1$ that meets $\mathcal{L}$ in a point. By labelling the points on the spaces Πj carefully (see below) we ensure that the $t' - t + 1$ points on $\mathcal{L}$

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

defined by any t shareholders (one point on $\mathcal{L}$ for each space Πj) are all distinct, and hence together define $\mathcal{L}$. Thus the original scheme is a (t, n)-threshold scheme.

5. Each subshare is one point, the secret (and each share) is defined by $t' - t + 1$ points, and hence the scheme is optimal.

It remains to describe how to allocate the points on each space to shareholders in order to ensure the "distinctness" property described above. A summary of how this is done is as follows:

1. Let ξ be a Singer cycle on $\mathcal{L}$ (ξ permutes the points of $\mathcal{L}$ in a cycle whose length is the number of points on $\mathcal{L}$).

2. Extend ξ to an automorphism ϕ of $\Pi 1$.

3. Let the points on $\Pi 2$ be a projection of the points on $\Pi 1$. If shareholder i received point Xi on $\Pi 1$ then give shareholder i the projection of point $\phi(Xi)$ on $\Pi 2$.

4. More generally, let the points on $\Pi(j+1)$ be a projection of the points on $\Pi 1$. If shareholder i received point Xi on $\Pi 1$ then give shareholder i the projection of point $\phi^j(Xi)$ on Πj.

The linearity relationships between the points on $\Pi 1$ are preserved by the automorphism ϕ and so the resulting configuration on $\Pi 2$ has the same properties as that on $\Pi 1$. Further, as ϕ restricted to $\mathcal{L}$ is ξ, we are guaranteed that the there are no points on $\mathcal{L}$ fixed by ϕ. Hence (considering the simple example) if points $X1, Y1$ generate point $Z1$ on $\mathcal{L}$, then points $\phi(X1), \phi(Y1)$ generate line $\phi(Z1)$ on $\mathcal{L}$, with $\phi(Z1)$ distinct from $Z1$. A similar argument applies to the other spaces Πj since ϕ^j is also an automorphism of $\Pi 1$ that fixes $\mathcal{L}$. It is interesting to note that the optimal geometrical construction can be used to reduce the amount of information which needs to be delivered to the combiner if we allow the threshold of participants who submit their (partial) shares to be increased. For example, in our optimal $(2, n)$ threshold changeable scheme, if two participants want to reconstruct the secret, they have to send their full shares (two points for each) to the combiner and the total amount of information is $2H(S)$. If three participants send their partial shares (one point for each), they can still recover the secret, but the total information delivered to the combiner is reduced to $1.5H(S)$.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

5 Changing Threshold of an Arbitrary Threshold Scheme

We close by considering the problem of changing the threshold parameter of an arbitrary (t, n) threshold scheme, without dealer assistance or secure links. Thus we cannot guarantee that subshares can be deterministically derived from the original shares, as in the previous section. In reality this problem seems very difficult to solve with any degree of satisfaction, however we suggest two possible methods which could be further developed in a search for a solution. Both techniques involve releasing information about shares, instead of shares themselves.

5.1 Changing Thresholds via Probabilistic Shares

Instead of submitting shares to a combiner, this first idea is that participant give away some "hints" about their shares. This hint specifies a subset of values to which the share belongs (specification of particular bits, for example). Thus the information provided by P_i about the share s_i takes the form of a set $\mathcal{B}_i$ such that $s_i \in \mathcal{B}_i$. One approach to reconstruction is as follows. When trying to reconstruct the secret, each P_i submits their set (hint) $\mathcal{B}_i$ $(i = 1, \ldots, \ell)$ to the combiner. The combiner groups the sets into collections of size t, and from each such collection derives the set of all possible secrets corresponding to all the possible share allocations using these share hints. Using the following hints, and the corresponding possible secret sets S^i,

$$\begin{aligned} \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}, \mathcal{B}_t &\rightarrow \quad S^t \\ \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}, \mathcal{B}_{t+1} &\rightarrow \quad S^{t+1} \\ &\vdots \\ \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}, \mathcal{B}_\ell &\rightarrow \quad S^\ell \end{aligned}$$

the combiner can then precisely recover the secret if $|S^t \cap S^{t+1} \cap \ldots \cap S^\ell| = 1$. It is however clear that such a solution cannot guarantee the precise new value of the threshold. An open problem is thus to determine methods of selecting hints in order to be able to specify within a certain probability that the secret can be reconstructed uniquely.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

5.2 Combiner Assisted Threshold Change

To avoid the uncertainty of the probabilistic method it is necessary to find a deterministic analogue of the probabilistic sharing idea. This may be possible if information about shares in a threshold scheme can be deterministically released in some manner. An idea is to negotiate a common encoding for delivery of information about participants' shares. The following provides an illustration of how this might work. Assume the original scheme is a (t, n) Shamir scheme based on polynomial $f(x)$ over GF(q) of degree at most $t-1$. As usual a participant P_i; $i = 1, \ldots, n$ is assigned a public co-ordinate x_i and a share $s_i = f(x_i)$. The secret is $s = f(0)$. It is well-known that any t participants can collectively recover the secret as they can write t linearly independent equations and solve them. Let these t participants be $P_1, \ldots, P_t$, then they (or the combiner) can write

$$\begin{aligned} s_1 &= f(x_1) = a_0 + a_1 x_1 + \ldots + a_{t-1} x_1^{t-1} \\ &\vdots \\ s_t &= f(x_t) = a_0 + a_1 x_t + \ldots + a_{t-1} x_t^{t-1} \end{aligned}$$

Let the combiner impose the encoding scheme such that every integer $c_i \in GF(q)$ is represented as a vector of k co-ordinates so

$$c_i = c_{i,0} + b c_{i,1} + b^2 c_{i,2} + \ldots + b^{k-1} c_{i,k-1} = (c_{i,0}, \ldots, c_{i,k-1})$$

where b is the base (for binary representation $b = 2$). We assume that the representation is one to one. Note that if we encode s_i and a_j; $j = 1, \ldots, t-1$ then from the equation

$$s_i = f(x_i) = a_0 + a_1 x_i + \ldots + a_{t-1} x_i^{t-1}$$

we get a system of k independent and equivalent equations related to the corresponding co-ordinates. Now the combiner can ask participant P_i to use the base b to determine the required representation of their share. If the new threshold is t' ($t' > t$), the combiner requests α subshares $s_{i,j}$; $j = 1, \ldots, \alpha$ such that

$$t' \times \alpha = t \times k$$

and the system of linear equations has a unique solution for vectors $a_i = (a_{i,0}, \ldots, a_{i,k-1})$. The combiner must get $t \times k$ linear equations and all $t \times k$ unknowns $a_{i,j}$ ($i = 0, \ldots, t-1$ and $j = 0, \ldots, k-1$) must be "covered". The

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

role of the combiner is to ask the participants for "right" subshares so the combiner can cover all unknowns. The presented method can be applied in all linear secret sharing schemes. The encoding may be based on any vector space.

6 Conclusions

In this paper we considered the problem of changing threshold when there is no secure channel to be used for the purpose of threshold change. One of the main motivation for this study was to provide robustness in a system where communication channels to the combiner have been tapped. We gave a number of constructions of threshold changeable schemes, including one that is optimal with respect to storage and communication costs. We made some initial remarks on the interesting problem of enabling the threshold of an arbitrary threshold scheme to be changed. Finding efficient and practical solutions to this latter problem remains open. We acknowledge useful discussions with Christine O'Keefe and Peter Wild concerning the design and correctness of the geometric construction.

References

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

[2] B. Blakley, G.R. Blakley, A.H. Chan and J. Massey. Threshold schemes with disenrolment. *Advances in Cryptology – CRYPTO '92, Lecture Notes in Comput. Sci.*, 740:540–548, 1993.

[3] G. R. Blakley and C. Meadows. Security of ramp schemes. *Advances in Cryptology – Proceedings of CRYPTO '84, Lecture Notes in Comput. Sci.*, 196:242-268, 1985.

[4] C. Blundo, A. Cresti, A. De Santis and U. Vaccaro. Fully dynamic secret sharing schemes. *Advances in Cryptology – CRYPTO '93, Lecture Notes in Comput. Sci.*, 773:110–125, 1993.

[5] R. Capocelli, A. Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Advances in Cryptology - CRYPTO '91, Lecture Notes in Comput. Sci.*, 576:101–113, 1992. also, Journal of Cryptology, vol. 6, no. 3, pp. 157-167, 1993.

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.

[6] Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(41):449–457, 1994.

[7] Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. *Preprint.*

[8] W.-A. Jackson and K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.*, 4:83-95, 1994.

[9] W.-A. Jackson and K.M. Martin. A combinatorial interpretation of ramp schemes. *Australasian Journal of Combinatorics*, 14:51–60, 1996.

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

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

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

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

[14] K.M. Martin, R.Safavi-Naini and H.Wang. Bounds and techniques for efficient redistribution of secret shares to new access structures. *Preprint.*

[15] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[16] G. Simmons. How to (really) share a secret. *Advances in Cryptology – CRYPTO '88, Lecture Notes in Comput. Sci.*, 403:390–448, 1990.

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

Appeared in *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999)*, Lecture Notes in Computer Science 1587, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (eds.), Springer-Verlag, pp. 177–191, 1999.