The Detection of Cheaters in Threshold Schemes

E. F. Brickell
Sandia National Laboratories
Albuquerque, NM 87185

D. R. Stinson
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2 Canada

Abstract

Informally, a (t, w)-*threshold scheme* is a way of distributing partial information (*shadows*) to w participants, so that any t of them can easily calculate a *key* (or *secret*), but no subset of fewer than t participants can determine the key. In this paper, we present an unconditionally secure threshold scheme in which any cheating participant can be detected and identified with high probability by any honest participant, even if the cheater is in coalition with other participants. We also give a construction that will detect with high probability a dealer who distributes inconsistent shadows (shares) to the honest participants. Our scheme is not perfect; a set of $t-1$ participants can rule out at most $1 + \binom{w-t+1}{t-1}$ possible keys, given the information they have. In our scheme, the key will be an element of GF(q) for some prime power q. Hence, q can be chosen large enough so that the amount of information obtained by any $t-1$ participants is negligible.

1. Introduction

Informally, a (t, w)-*threshold scheme* is a way of distributing partial information (*shadows*) to w participants, so that any t of them can easily calculate a *key* (or *secret*), but no subset of fewer than t participants can determine the key. Threshold schemes are also known as *secret sharing schemes*. A *perfect* threshold scheme is one in which no subset of fewer than t participants can determine any partial information regarding the key.

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 564-577, 1990.

Threshold schemes were first described independently by Blakley [2] and Shamir [7] in 1979. Since then, many constructions have been given for threshold schemes. More recently, various researchers have considered the problem of guarding against the presence of cheaters in threshold schemes. It is conceivable that any subset of the participants may attempt to *cheat*, that is, to deceive any of the other participants by lying about the shadows they possess. There is also the possibility that the person distributing the shadows (the *dealer*) may attempt to cheat. The dealer might distribute an inconsistent set of shadows, so that the key cannot be determined correctly, or so that different subsets of t participants would calculate different keys from the shadows they possess. If this is done without the knowledge or co-operation of any of the participants, we refer to this form of cheating as *disruption*. However, if this cheating is done in co-operation with one or more of the participants, we call it *collusion*.

A threshold scheme is said to be *unconditionally secure* (against cheating) if the probability of cheating successfully is independent of the computational resources available to the cheaters. Under the assumption that the dealer is honest, several constructions have been given for threshold schemes which are unconditionally secure against cheating [3, 6, 8, 9]. We now briefly summarize the properties of these threshold schemes.

As far as the authors are aware, the first researchers to address the problem of cheaters in threshold schemes were McEliece and Sarwate in [6]. They use an error-correcting code to construct a threshold scheme in which any group of $t + 2e$ participants which includes at most e cheaters can correctly calculate the key.

Tompa and Woll [9] proceed as follows. The dealer specifies a subset K_0 of the set of possible keys K. A key will be accepted as authentic only if it is an element of K_0. If a set of t participants calculate the key to be an element of $K \setminus K_0$, then they realize that one of them is cheating. The probability of successful cheating is at most $1 - |K_0| / |K|$, even if $t-1$ participants conspire to to cheat another participant. However, even though participants can detect when cheating has occurred, they cannot determine who is cheating.

The construction of Simmons [8] is more general, in that it can be applied to most existing threshold schemes. This method detects cheating only if at least $t + 1$ participants exchange their shadows. Define a set S of at least t shadows to be *consistent* if all t-subsets of S determine the same key. Then, a key is accepted as authentic only if there is a consistent subset of at least $t + 1$ shadows which determine it. If $t + e$ participants exchange shadows and there are at most $e - 1$

cheaters among them, then they possess a consistent subset of at least t + 1 shadows. Unfortunately, the only known method to determine the existence of a consistent set of t + 1 shadows is an exhaustive search.

Finally, Chaum [3] has suggested the following approach. For *each* bit b to be communicated to the ith participant, the dealer chooses 2w – 2 large random numbers r_{j0} and r_{j1} ($1 \le j \le w, j \ne i$). For each j, r_{j0} and r_{j1} are given to participant j. The dealer gives to the ith participant the bit b and all r_{jb} ($1 \le j \le w, j \ne i$). Then, r_{jb} is used to authenticate the bit b (as 0 or 1, respectively) to participant j. This procedure is used for every bit communicated to each participant.

In the schemes discussed above, it is assumed that the dealer is honest. Also, the Tompa and Woll scheme and the Simmons construction require that the participants be able to simultaneously release their shadows, in order to ensure that no participant is able to obtain partial information about the shadows of the other participants before releasing his own shadow. Simultaneous release of shadows is *not* required in the Chaum scheme.

Threshold schemes which provide protection against dealer disruption have been presented by Chor, Goldwasser, Micali and Awerbuch in [5] and by Benaloh in [1]. These schemes provide *computational security* only, since they rely on computational assumptions regarding certain encryption schemes. Chaum, Crepeau and Damgard [4] use threshold schemes as a building block in unconditionally secure multiparty protocols. They tolerate both dealer disruption and collusion, but require that less than one third of the participants cheat. Under these assumptions, they describe a scheme that is unconditionally secure and which allows the key to be determined correctly by the honest participants.

The threshold scheme we present provides unconditional security and gives the honest participants the ability to *identify* cheaters, assuming the dealer is honest. Also, we do *not* require that the participants simultaneously release their shadows. The properties of our construction can be summarized as follows.

1) The key is an element of GF(q), and each shadow is a t-dimensional vector over GF(q) (q will be some large prime power).

2) Any participant who attempts to cheat will be identified by any honest participant with probability $1 - 1 / (q - 1)$.

3) Even if there is only one honest participant and the remaining $w - 1$ participants form a coalition in order to deceive him, their probability of cheating successfully is only $(w - t + 1) / (q - 1)$.

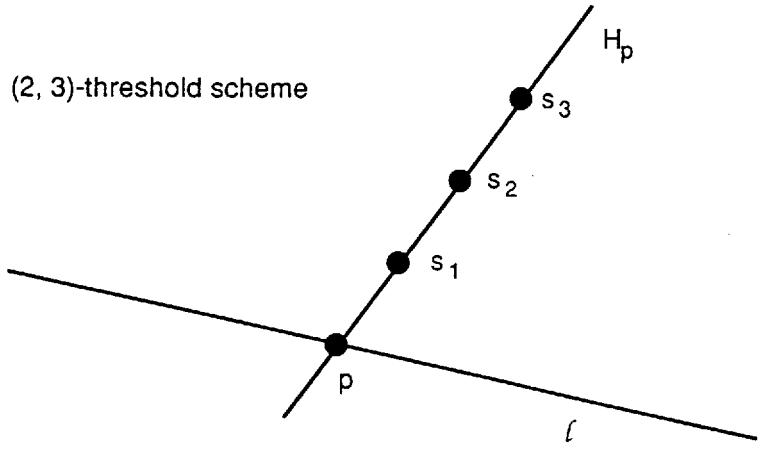
4) The scheme is nearly perfect. A group of $t - 1$ participants can eliminate at most $1 + \binom{w - t + 1}{t - 1}$ possible keys, and can obtain no other partial information about the key. If q is large, this will cause no difficulty in practice.

5) The scheme can also protect against dealer disruption, by using a "cut-and-choose" technique similar to that of [4].

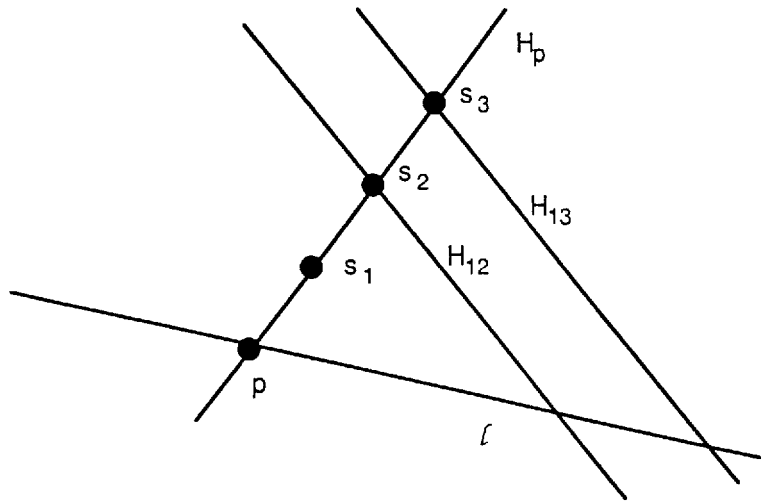
2. The construction

Our construction is a modification of Blakley's threshold scheme [2], which we now review briefly. Suppose the participants are denoted A_i, $1 \le i \le w$, and the dealer is denoted by D. Let V be a t-dimensional vector space over GF(q), where q is some large prime power. First, D fixes a line ℓ in V. This line is made known to all the participants. There are q possible keys, namely the q points on ℓ. If D wants to distribute shadows corresponding to a key p, he first constructs a random $(t - 1)$-dimensional subspace H that meets ℓ in a point. Then, he constructs the hyperplane $H_p = H + p$. (Note that $H_p \cap \ell = p$.) Finally, he picks w random points on H_p, denoted s_i $(1 \le i \le w)$, such that the points in the set $\{p\} \cup \{s_i: 1 \le i \le w\}$ are in general position (that is, no j of them lie on a flat of dimension $j - 2$, if $j \le t$). The point s_i is the shadow that D gives to A_i.

Any t participants can uniquely determine the hyperplane H_p, and then obtain p by calculating $H_p \cap \ell = p$. However, a subset of t' $(< t)$ participants know only that H_p contains the flat F of dimension $t' - 1$ generated by the shadows they possess. For any p' on ℓ, there is a hyperplane H_p containing F and p'. Hence, they have no information as to the point p. Thus, the scheme is indeed a (t, w)-threshold scheme.



In order to guard against cheating, we modify the threshold scheme. D will distribute extra information to the participants, along with the shadows. For ease of exposition, we first discuss the case t = 2. In this case, H is a 1-dimensional subspace and the hyperplane H_p is a line. D constructs w random 1-dimensional subspaces, denoted H_i ($1 \le i \le w$), each of which is distinct from H. We do *not* require that the subspaces H_i ($1 \le i \le w$) be distinct. D gives to each A_j the $w - 1$ parallel lines $H_{ji} = H_j + s_i$, $1 \le i \le w$, $i \ne j$. These lines H_{ji} are called *supershadows*. Note that H_{ji} is given only to A_j.

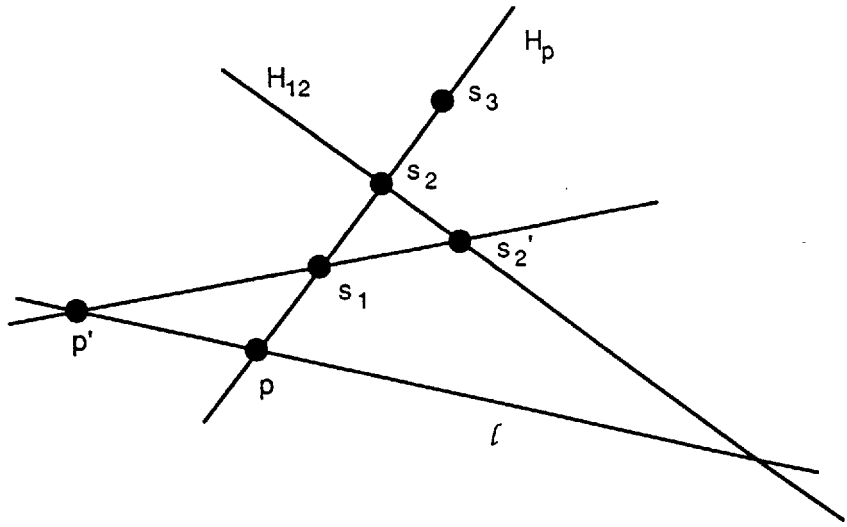


We must first show that knowledge of the supershadows does not enable any one participant to determine the key. Let's consider A_1. He knows that $s_2 \in H_{12}$. This *does* give him some partial information, namely that the key $p \neq H_{12} \cap \ell$. For, if $p = H_{12} \cap \ell$, then $p = s_2$, which is not allowed. Similarly, A_1 knows that $p \neq H_{1i} \cap \ell$, for any i, $2 \leq i \leq w$. As well, $p \neq H_{11} \cap \ell$, where H_{11} denotes the line through s_1 parallel to the H_{1i}'s. For, this would require that $H_p = H_{11}$, but $s_2 \notin H_{11}$. Thus, A_1 has ruled out w possibilities for p. However, the key, p, could be any point p_0 on ℓ other than these w points, since the line $p_0 s_1$ will intersect each H_{1i} in a point. Each of these $q - w$ possibilities for p is equally likely to occur.

Hence, each participant can rule out w possibilities for the key, and knows that the key is equally likely to be one of the $q - w$ remaining possibilities. Thus, the scheme is no longer perfect. However, if q is large relative to w, this will cause no difficulty in practice. (A variation of this scheme, described in Section 4, allows only one possible value to be ruled out for the key in the case $t = 2$.)

Next, we consider the possibility that certain participants will cheat, by lying as to what shadows they possess. In the worst case, $w - 1$ participants, say A_i $(2 \leq i \leq w)$ will form a coalition in order to try to convince A_1 that the key is some value $p' \neq p$. We will assume that $w \geq 3$, so that the coalition can determine the line H_p and the key p before attempting to deceive A_1. Note that they can also calculate s_1, since $s_1 = H_p \cap H_{21}$, for example.

Suppose A_2 tells A_1 that his shadow is some point s_2' rather than s_2. A_2 will not choose s_2' to be any point on ℓ, or any point on the line through s_1 parallel to ℓ, since A_1 would then realize that A_2 is lying. Also, A_2 will not choose s_2' to be a point on H_p, since this would not deceive A_1 as to the value of p. Hence, he will choose s_2' to be one of the remaining $q^2 - 3q + 2$ points. For any such choice of s_2', there is a unique line H_{12}' joining s_2' and s_2. A_1 will be deceived if and only if $H_{12}' = H_{12}$. Since $H_{12} \neq H_p$, there are $q - 1$ possibilities for H_{12}, all equally likely. Each of these $q - 1$ lines through s_2 contains $q - 2$ of the $q^2 - 3q + 2$ points mentioned above. Thus, the chance that A_2 deceives A_1 is $1 / (q - 1)$.



If all the other A_i ($2 \le i \le w$) independently try to deceive A_1 in a similar fashion, the probability that at least one of them succeeds is

$$1 - \left(1 - \left(\frac{1}{q-1}\right)\right)^{w-1} \le \frac{w-1}{q-1}.$$

Their best strategy is to conspire; if they ensure that no two of the lines $s_i's_i$ are parallel, then A_1 will be deceived by one of them with probability equal to $(w-1)/(q-1)$. This will be a negligible quantity if q is large compared to w.

If $w = 2$, then the analysis is slightly different. Suppose A_2 attempts to deceive A_1. If A_2 can obtain the value of s_1, then the arguments proceed as before, and A_2 can deceive A_1 with probability $1/(q-1)$. (This could happen if A_1 reveals s_1 to A_2 before A_2 reveals s_2 to A_1, for example.) If A_2 cannot obtain the value of s_1, then his probability of deceiving A_1 is decreased to $1/q$, since he might choose s_2' to be a point on H_p.

Let's now consider the general case $t \ge 3$. Recall that H is a $(t-1)$-dimensional subspace and H_p is a hyperplane. D constructs w random $(t-1)$-dimensional subspaces, denoted H_i ($1 \le i \le w$). We require that the intersection of H with $j-1$ of these H_i's is a subspace of dimension $t-j$, if $j \le t$. (In the case $t = 2$, this condition reduces to the previous requirement that the H_i's ($1 \le i \le w$) be distinct from H.) The $w-1$ supershadows D gives to each A_j are the parallel hyperplanes $H_{ji} = H_j + s_i$, $1 \le i \le w$, $i \ne j$.

One way to select the H_i's is as follows. First, choose w subspaces of H, denoted K_i $(1 \le i \le w)$, each of dimension $t-2$, in general position. Then select w points not in H, denoted q_i $(1 \le i \le w)$. These points need not be distinct. Finally, define H_i to be the subspace spanned by K_i and q_i $(1 \le i \le w)$.

First, we show that knowledge of the supershadows does not enable any $t-1$ participants to determine the key. Suppose that participants A_i, $1 \le i \le t-1$, attempt to determine the key. They know that H_p contains F, the $(t-2)$-dimensional flat generated by $s_1, \ldots, s_{t-1}$. They know also that a shadow s_j $(t \le j \le w)$ occurs on the line ℓ_j which is the intersection of the H_{ij}, $1 \le i \le t-1$. (Since ℓ_j meets H_p in a point, it has dimension one and is indeed a line.) Notice that any two of these lines ℓ_j are parallel, since the hyperplanes H_{ij} are parallel (for any fixed i).

We claim that for any j, $t \le j \le w$, ℓ_j and F generate the whole n-dimensional space (consequently, $\ell_j \cap F = \varnothing$). This is seen as follows. Suppose ℓ_j and F are contained in some hyperplane H', for some j, $t \le j \le w$. Since $s_j \in \ell_j$ and $s_1, \ldots, s_{t-1} \in F$, $H' = H_p$. Then $\ell_j \subseteq H_p \cap H_{1j} \cap H_{2j} \cap \ldots \cap H_{(t-1)j}$. It follows that $H \cap H_1 \cap H_2 \cap \ldots \cap H_{(t-1)}$ has dimension at least one, which is ruled out by the way in which the hyperplanes H_i were chosen.

Next, we observe that $F \cap \ell = \varnothing$. It is impossible that $\ell \subseteq H_p$ since $H_p \cap \ell = \{p\}$ and $F \subseteq H_p$. Also, F and ℓ cannot intersect in a point, for this point would have to be p, which would contradict the requirement that the shadows are in general position with respect to p.

It is now easy to verify that there is a unique point p' on ℓ such that the hyperplane determined by F and p' is parallel to each ℓ_j, $t \le j \le w$. Then, the key $p \ne p'$. For, if $p = p'$, then $H_p \cap \ell_j = \varnothing$; but $s_j \in H_p \cap \ell_j$, a contradiction. This enables the participants A_i $(1 \le i \le t-1)$ to rule out one possible value for the key.

There are in fact other points that can be ruled out as possible values for the key. We saw earlier that when t = 2, the w − 1 points $\ell \cap \ell_j$ ($t \le j \le w$) can also be eliminated as possible values for p. In general, the number of possible keys that can be ruled out (other than the point p') is $\binom{w-t+1}{t-1}$.

We can see this as follows. Let $j_1, \ldots, j_{t-1}$ be distinct integers such that $t \le j_i \le w$ ($1 \le i \le t-1$), and let U be the flat spanned by the ℓ_{j_i} ($1 \le i \le t-1$). Since the lines ℓ_j are all parallel, U has dimension at most $t-1$. The flat T spanned by the points s_{j_i} ($1 \le i \le t-1$) has dimension $t-2$, and is contained in $U \cap H_p$. As well, $\ell_j \cap H_p = \{s_j\}$, for any j, $t \le j \le w$. It follows that the dimension of U is exactly $t-1$ and $T = U \cap H_p$.

Next, we observe that it is impossible that $\ell \subseteq U$. Since $\ell \cap H_p = \{p\}$, this would force $p \in T$. But then the $t-1$ shadows $s_{j_1}, \ldots, s_{j_{t-1}}$ and p would then be contained in the flat T having dimension at most $t-2$. Hence, either $\ell \cap U$ is empty, or $\ell \cap U$ is a point, say r. In the latter case, r cannot be the key, since (as before) the $t-1$ shadows $s_{j_1}, \ldots, s_{j_{t-1}}$ and r would then be contained in the flat T. Hence, it is possible that $t-1$ participants can rule out as many as $1 + \binom{w-t+1}{t-1}$ possible values for the key.

Example: Suppose we have a (3, 5)-threshold scheme over GF(q), for some large prime q. Suppose ℓ is the line (b, 0, 0) ($b \in$ GF(q)), $s_1 = (1, 1, 2)$ and $s_2 = (1, 1, 6)$. Thus, F is the line (1, 1, b) ($b \in$ GF(q)). Suppose also that ℓ_3 is the line ($1 + a$, $3 - a$, 2) ($a \in$ GF(q)), ℓ_4 is the line ($1 + a$, $-a$, 1), and ℓ_5 is the line ($8 + a$, $-a$, 3) (these three lines are parallel, having direction vector (1, −1, 0)). A_1 and A_2 would analyze the situation as follows. Suppose the key is $p = (x_0, 0, 0)$. Then, H_p is the plane $x + y(x_0 - 1) = x_0$. This plane intersects ℓ_3, ℓ_4, and ℓ_5 if and only if $x_0 \ne 2$. Thus, (2, 0, 0) is ruled out as the key. Three other points can also be ruled out. For example, ℓ_3 and ℓ_4 generate the plane U having equation $x + y - 3z = -2$. U meets ℓ in the point (−2, 0, 0). If −2 were the key, then H_p would have equation $x - 3y = -2$. Hence, it would follow that $s_3 = (5 / 2, 3 / 2, 2)$ and $s_4 = (1 / 4, 3 / 4, 1)$ (all arithmetic being done in GF(q)). Then s_3, s_4, and p are all collinear, a contradiction. In a similar manner, −4 is ruled out by consideration of ℓ_3 and ℓ_5, and −5 / 2 is eliminated by consideration of ℓ_4 and ℓ_5.

The last topic we examine in this section is the probability of successful cheating. Suppose $w - 1$ participants, say A_i $(2 \le i \le w)$ form a coalition in order to try to convince A_1 that the key is some value $p' \neq p$. Their best strategy is to leave $t - 2$ of their shadows unchanged, and lie about the remaining $w - t + 1$ shadows. The probability that A_1 will detect that any particular shadow is a forgery is $1 / (q - 1)$, as in the $t = 2$ case. The chance that A_1 is fooled by at least one of the $w - t + 1$ altered shadows is at most $(w - t + 1) / (q - 1)$.

3. A cut-and-choose procedure to eliminate dealer disruption

We can eliminate the possibility of the dealer disruption by using a *cut-and-choose* procedure, as in [4] and [1]. Let K be some security parameter (say $K = 50$). Suppose H_p is the hyperplane $ax^T = c$, where the superscript "T" denotes transpose. The following protocol will be repeated K times.

1. D generates a random non-singular matrix M and a random t-tuple b. D then computes $s_i' = s_iM^T + b$ and gives s_i' to A_i, $1 \le i \le w$. (So, the s_i' are obtained from the s_i by a random affine transformation.)

2. Depending on a coin flip f, D performs a) or b).

   a) if f = "heads", then D reveals M and b, and each A_i verifies that $s_i' = s_iM^T + b$.
   b) if f = "tails", then D computes $a' = aM^{-1}$ and $c' = c + a'b^T$, and reveals a' and c'. Then, each A_i verifies that $a'(s_i')^T = c'$.

If the dealer can answer *both* challenges a) and b), then it must be the case that $c = as_i^T$, $1 \le i \le w$. That is, the shadows all lie on a hyperplane. If the dealer attempts to cheat, he can answer only one of the two challenges in any given round of the protocol. Hence, the probability of the dealer fooling any given set of t honest participants after K rounds is 2^{-K}.

It is also easy to see that no information is revealed to the participants by this protocol. If operation 2a) is performed in any round of the protocol, then the participants learn only the affine transformation used in that round. This is of no use in determining the key. If 2b) is performed, then the participants obtain the

hyperplane $a'x^T = c'$. This tells them nothing about H_p, since any hyperplane can be mapped to any other hyperplane by means of an affine transformation.

Notice that we require the existence of a *broadcast channel* in step 2) of this protocol. This is a channel in which it is guaranteed that every participant receives the *same* information from the dealer (i.e. the values of M and b in 2a); or a' and c' in 2b)). If a broadcast channel is not used, then the dealer could attempt to cheat during this protocol by giving different information to different participants.

We can also do a cut-and-choose procedure on the supershadows. Here, the object is to convince each participant A_i that $s_j \in H_{ij}$, $i \neq j$, without revealing s_j. Suppose the hyperplane H_{ij} is given by the equation $a_i \cdot x = b_{ij}$, $1 \leq i, j \leq w$, $i \neq j$. The following protocol will be repeated K times.

1. For $1 \leq j \leq w$, D generates a random t-tuple s_j', and gives s_j' to A_j. D then computes $b_{ij}' = a_i \cdot s_j'$ and gives b_{ij}' to A_i, $1 \leq i, j \leq w$, $i \neq j$.

2. Depending on a coin flip f, D performs a) or b).

   a) if f = "heads", then D reveals all s_j', $1 \leq j \leq w$, and each A_i verifies that $b_{ij}' = a_i \cdot s_j'$.
   b) if f = "tails", then D reveals all $s_j + s_j'$, $1 \leq j \leq w$, and each A_i verifies that $a_i \cdot (s_j + s_j') = b_{ij} + b_{ij}'$, $1 \leq j \leq w$.

The analysis of dealer disruption is similar to the previous situation. If the dealer can answer *both* challenges a) and b) in any given round of the protocol, then it must be the case that $a_i \cdot s_j = b_{ij}$, $1 \leq i, j \leq w$, $i \neq j$. That is, the shadow s_j lies on the hyperplane $a_i \cdot x = b_{ij}$. As before, the probability of the dealer fooling any t honest participants in all K rounds is 2^{-K}.

Next, we consider whether any information about the shadows is released by this protocol. As before, if operation 2a) is performed in any round of the protocol, then clearly no information about the shadow is released. If operation 2b) is done, then A_i learns all values $s_j + s_j'$, but this tells him nothing about any s_j.

Finally, observe that we require a broadcast channel in step 2), as in the previous protocol.

Although the protocol protects against dealer disruption, we cannot guard against collusion of the dealer and any participant. For suppose D colludes with participant A_1. D can tell A_1 all the supershadows H_{i1}, and all the shadows s_i, $2 \le i \le w$. No collusion can be detected in the cut-and-choose procedure, since A_1 never reveals any information. Then, suppose a group of t participants including A_1, say $\{A_i: 1 \le i \le t\}$, attempt to determine the key. A_1 can compute the intersection ℓ_1 of the $t-1$ hyperplanes H_{i1}, $2 \le i \le t$. Note that ℓ_1 is a line. If A_1 claims that his shadow is any point on ℓ_1 other than s_1, then the other $t-1$ participants will not detect that he is cheating, and they will calculate an incorrect key. In this way, A_1 can make the other $t-1$ participants believe the key is any value he desires.

4. Remarks

There are many variations of this threshold scheme. For example, the threshold scheme could be implemented in a projective space rather than in an affine space. In the case t = 2, less partial information is revealed in a projective setting. D would fix a line ℓ in a projective plane P. As before the key p would be a point on ℓ. D also picks a random line H intersecting ℓ in p, and distribute points on $H \setminus \{p\}$ as the shadows. Supershadows are obtained as follows. For each participant A_i, D picks a point $q_i \in \ell \setminus \{p\}$ (these points need not be distinct). The supershadow H_{ij} is the line $s_j q_i$. With supershadows defined in this way, each participant A_i can only rule out the point q_i as the key (note that A_i can compute q_i as the intersection of any two of the supershadows he possesses).

It is an interesting open question to determine if there is a *perfect* threshold scheme satisfying all the other properties of our scheme (i.e. one in which *no* possible keys can be ruled out).

Another question is the amount of computation required. The dealer must verify certain conditions, including that the shadows are in general position. This is not difficult for small t and w, but could require a lot of time if t and w are large. Is there a scheme which is still computationally efficient for large t and w? (Note that the Shamir scheme [7] *is* computationally efficient; but it is not clear how to modify it to detect cheating.)

Yet another issue is the amount of (secret) information that needs to be communicated, in the form of shadows and supershadows. We ask if a scheme can be constructed which requires less information to be distributed.

Finally, we ask if it is possible to construct a threshold scheme that provides unconditional security against collusion of the dealer and one or more participants.

Acknowledgements

This research was discussed with David Chaum and his colleagues at C. W. I. We would like to thank them for their helpful observations and comments. Thanks also to Marijke De Soete for useful comments.

Added in proof

After writing this paper, we discovered that Tal Rabin was working independently on a related problem. Her results were presented at CRYPTO '88, in a paper entitled "Robust sharing of secrets when the dealer is honest or cheating". The techniques she employs can also be used to solve the problem we consider in our paper. Our approach requires that less secret information be communicated, but is slightly less efficient computationally.

References

1. Josh Cohen Benaloh, *Secret sharing homomorphisms: keeping shares of a secret secret*, Advances in Cryptology – CRYPTO 86 Proceedings, pp. 251-260, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, Berlin, 1987.

2. G. R. Blakley, *Safeguarding cryptographic keys*, Proc. N. C. C., vol. 48, AFIPS Conference Proceedings 48 (1979), 313-317.

3. David Chaum, personal communication.

4. David Chaum, Claude Crepeau and Ivan Damgard, *Multiparty unconditionally secure protocols*, to appear in Proceedings of the 20th ACM Symposium on the Theory of Computing, 1988.

5. B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, *Verifiable secret sharing and achieving simultaneity in the presence of faults*, Proc. 26th IEEE Symp. on Foundations of Computer Science, 1985, 383-395.

6. R. J. McEliece and D. V. Sarwate, *On sharing secrets and Reed-Soloman codes*, Comm. of the ACM 24 (1981), 583-584.

7. A. Shamir, *How to share a secret*, Comm. of the ACM 22, (1979), 612-613.

8. G. Simmons, *An introduction to shared secret schemes and their applications*, Sandia Report SAND88-2298, 1988.

9. M. Tompa and H. Woll, *How to share a secret with cheaters*, J. of Cryptology 1 (1988), 133-138