A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party*

Ingemar Ingemarsson
Linköping University
Department of Electrical Engineering
S-58183 Linköping, Sweden

Gustavus J. Simmons
Sandia National Laboratories
Albuquerque, New Mexico 87185, USA

Introduction

All shared secret or shared control schemes devised thus far are autocratic in the sense that they depend in their realization on the existence of a single party—which may be either an individual or a device—that is unconditionally trusted by all the participants in the scheme [5,6]. The function of this trusted party is to first choose the secret (piece of information) and then to construct and distribute in secret to each of the participants the private pieces of information which are their shares in the shared secret or control scheme. The private pieces of information are constructed in such a way that any authorized concurrence (subset) of the participants will jointly have sufficient information about the secret to reconstruct it while no unauthorized collection of them will be able to do so. For many applications, though, there is no one who is trusted by all of the participants, and in the extreme case, no one who is trusted by anyone else. In the absence of a trusted party or authority, no one can be trusted to know the secret and hence—until now—it has appeared to be impossible to construct and distribute the private pieces of information needed to realize a shared control scheme. It is worth noting that in commercial and/or internation(al) applications, this situation is more nearly the norm than the exception.

* This work performed in part at Sandia National Laboratories supported by the U. S. Department of Energy under contract no. DE-AC04-76DP00789.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 266-282, 1991.

The single exception is that a way has been known (and used) for several years to ensure unanimous consent before a controlled action can be initiated [7]. For example, if it is desired that a specific two persons (controllers) must concur in order for a vault to be opened (or a weapon enabled or a missile fired) then each of these controllers could—during the initialization of the locking mechanism in the vault door—enter a randomly chosen k-digit number whose value is kept secret by the controller who chose it. The mod 10 sum of these two private and secret k-digit numbers would be the secret k-digit combination needed to open the vault. The subsequent entry of any pair of k-digit numbers whose mod 10 sum is equal to the secret combination determined by the two controllers would open the vault door. Clearly the probability that an outsider or either of the two insiders (controllers) alone being able to open the vault on the first try would be 10^{-k}. In this control scheme, two controllers are involved, and both must (in probability) concur in order for the controlled event to be initiated. For anything other than a unanimous consent scheme, however, a functional dependence must exist between the participants' private pieces of information reflecting the structure of the authorized concurrences—even though the participants don't trust each other so that cooperation in achieving such a dependence can't be assumed. In this paper we present a protocol to set up shared control schemes without the assistance of any trusted party, in which participants need only act in their own self interest.

The problem of setting up shared secret schemes in the absence of a trusted third party has been largely ignored by researchers in this area—with the single exception of a paper by Meadows [4]. In it she discusses this problem and at even greater length the twin questions of how new participants can be enrolled in an already existing shared control scheme and of how previously enrolled participants can be cut out. To accomplish this, she uses a construction which she calls a rigid linear threshold scheme that makes it possible for a predetermined number of the existing participants to delegate their capability to a new member—essentially to vote him into membership. Her constructions do not appear to be related to the approach to be presented here, especially so since her primary proposal depends on a secure (unconditionally trustworthy) black box to replace the services of an unconditionally

ally trustworthy key distribution center. Meadows attributes the question of whether a shared secret scheme can be set up without the assistance of a trusted key distribution center to Chaum, however the paper of his that she cites—"Some Open Questions"—did not appear in the Proceedings for Crypto'84 where she references it. The important point, though, is that her work appears to be the only prior reference to the problem of how a shared control scheme can be set up without the assistance of a trusted key (share) distribution center.

Democratic Shared Control Schemes

The essential notion to our protocol is that the secret (piece of information) will be jointly determined in a unanimous consent scheme from inputs made privately by each of the participants. Each of these inputs is to be equally influential in determining the value of the secret and will itself be kept secret by its contributor. Shared control schemes of this sort in which each participant has an equal influence on the determination of the secret (i.e., the information equivalent of the democratic principal of "one man-one vote") will be referred to as democratic (schemes) as contrasted to autocratic schemes in which the participants have no input to the initial determination of the secret (information). Once the secret has been determined, each participant may, if he wishes, devise private shared control schemes with which to distribute among the other participants private pieces of information that would make it possible for some groupings of them to reconstruct his contribution to the determination of the secret.

To summarize, the general protocol with which a group of mutually distrustful participants can set up a democratic shared control scheme that they must logically trust—without the assistance of any outside party is:

1. The participants first set up a democratic unanimous consent scheme; i.e., one in which
   a) they each contribute equally to the determination of the secret (piece of information), and
   b) all of their private inputs (contributions) must be made available in order for the secret to be reconstructed.

2. After the unanimous consent scheme is in place, any of the participants who trust some concurrence(s), i.e., subsets of the other participants, to faithfully represent their interests can then create private autocratic shared secret schemes to distribute information about the private (and secret) contribution they made to the determination of the overall secret among the members of those concurrences.

Step 1 doesn't require that anyone trust anyone else. After step 2 has been completed, any concurrence of participants who were intrusted with another participant's share in the unanimous consent scheme can act in the stead of that participant—and no collection of the participants that doesn't include one of these concurrences can do so. In setting up these private shared secret schemes each participant is acting as his own "trusted authority" to protect his own interests, so that he need trust no one else insofar as the delegation of the capability to act in his stead is concerned. In this way, each participant can guarantee that only concurrences that either include him as a member or else that include a subset of the other participants whom he trusts to represent his interests will be able to initiate the controlled action or to recover the shared secret. Since each participant acts similarly, the net result is that democratic shared control schemes of arbitrary complexity (of control) can be established which accurately reflect the placement of trust (or lack of it) by the participants in each other [1]. In other words, every shared control scheme that would be acceptable to the participants and which could be set up by a mutually trusted authority, can also be set up as a democratic scheme by the participants themselves without anyone having to accept a greater risk of their interests being abused than they would have had to accept in order for a trusted authority to set up the scheme instead.

Implementation

Given this protocol, the first question is how the initial unanimous consent scheme can be set up. We have only found two—inequivalent—ways this can be done; either way, of course, can serve as the starting point for setting up more complex schemes using the protocol described above. The first is simply a generalization of the example given earlier.

1. In a space whose cardinality is adequate for the concealment of the secret, i.e., in which the probability of selecting a randomly chosen secret (point) in a subsequent random drawing provides an acceptable level of security for the controlled action, each participant chooses at random a point as his contribution to the unanimous consent control scheme. During the initialization of the mechanism that implements the shared control, each of the participants secretly enters the point he has selected and the sum (vector, modular, exclusive-or, etc.) of all of the points becomes the jointly defined secret value. Since this procedure is an obvious generalization of Vernam encryption, the secret is unconditionally secure from discovery (or recovery) by any concurrence of fewer than all of the participants so long as the sum operation is an entropy preserving mapping. To see that this is true, consider the worst case scenario in which all but one of the participants conspire in an attempt to initiate the controlled action without the cooperation of the single missing participant. They can calculate the point which is the sum of all of their contributions, however, every point in the space is still equally likely to be the secret point depending on the point chosen by the missing participant. In other words, even in this worst case scenario, the best that the would-be cheaters can do is to "guess" at the value of the secret using a uniform probability distribution on all of the points in the space. Clearly, this is the best that can be achieved.
2. In an n-dimensional finite space, where n is the total number of participants in the scheme and the cardinality of the space is chosen such that the probability of randomly choosing a particular point (the secret) out of all of the points in a hyperplane of the space provides an adequate concealment for the secret, each participant randomly chooses a hyperplane as his private contribution to the determination of the secret. The secret in this case is the point defined by the intersection of the n hyperplanes. With virtual certainty (as the number of points in

a hyperplane increases) the n independently chosen hyperplanes will intersect in only a single point. For example, consider the case of two lines in PG(2,q) or of three planes in PG(3,q). A pair of lines in PG(2,q) either intersect in a point or else they are coincident. The probability of this later occurring is $O(1/q^2)$. Similarly, there are only two ways three planes in PG(3,1) can have more than a point in common: either they are all three coincident or else they form a pencil of planes on a common line of intersection. The probability of these occurrences is $O(1/q^6)$ and $O(1/q^2)$, respectively.

The important point is that n hyperplanes in an n-dimensional space almost certainly (with q) intersect in only a single point, so that the protocol described here will almost certainly define a unique value for the secret. In the (unlikely) event that they do not for a particular choice of hyperplanes by the participants, this would be detected during the initialization phase of setting up the shared control scheme and the participants would then have to make another (random) choice of inputs.

We will refer to these two ways of realizing unanimous consent schemes as point and plane protocols, respectively. It might at first appear that the point and plane protocols are in some sense simply two versions of a single scheme; especially so in view of the geometric duality of points and hyperplanes and the fact that these objects are the private choices of inputs in the two protocols. It is easy, however, to show that this cannot be the case.

In the point protocol, the uncertainty about the secret is the same for an outsider as it is for every combination of fewer than all of the participants: namely it is equally likely to be any point in the containing space. Furthermore there is no relationship between the dimension of the space in which the secret is concealed and the number of participants in the shared control scheme. The only requirement is that the number of points in the space be large enough that the probability of choosing the secret (one) at random will be sufficiently small. In other words, a k-out-of-k scheme could be implemented in a 1-dimensional space as well as any other, even if the dimension of the containing space is greater than k.

On the other hand, in the plane protocol the dimension of the space must equal the total number of participants, say n. Otherwise the intersection of the n randomly and independently chosen hyperplanes will almost certainly over or under-determine a point; i.e., the hyperplanes will either not have a common point of intersection or else will intersect in a subspace of higher dimension. More importantly, though, outsiders and all proper subsets of the insiders will be faced with substantial differences in uncertainty about the secret. An outsider knows only that p is some point in PG(n,q), where all points are equally likely, i.e., an uncertainty about the secret of $O(q^{-n})$. Any single one of the participants, however, knows that p must be a point in the hyperplane he chose, i.e., a point in an (n-1)-dimensional subspace which is an uncertainty about p of only $O(q^{-(n-1)})$. Similarly, any pair of participants together could reduce the uncertainty about p to being a point in the (n-2)-dimensional flat which is the intersection of the two hyperplanes they chose, etc.

There are other, geometrical, arguments to show the inequivalence of these two protocols for setting up unanimous consent schemes in the absence of trust, but none so easy to see as this information based argument.

Given that the participants have set up a unanimous consent scheme (using either the point or the plane protocol) the next question is how each participant can then distribute shares in his input among concurrences of the other participants whom he trusts—if any exist. If the point protocol was used, so that each participant's input was a point, then conventional secret sharing schemes [5,6,7]—all of which are designed to control the recovery of a secret point—can be used. If the plane protocol was used, however, standard secret sharing schemes are not suitable, since the geometric object whose identification is to be shared is a hyperplane: not a point. To share a hyperplane requires that sets of subspaces (or varieties in general) be constructed such that the subsets of these held by trusted concurrences will suffice to determine the hyperplane, and no other subsets will do so. This may be easy. For example, if the plane protocol is used and the private hyperplanes are 3-dimensional, then it is easy to devise simple k-out-of-ℓ threshold schemes for k = 2, 3 or 4; the shares being a set of pairwise skew lines, a pencil of lines on a point—no three of which are coplanar, or a set of points—no four of which are coplanar, respectively. Note that only the first two cases are of interest, since the total number of participants in this case can only be four. On the other hand, it may be a difficult geometric problem. For example, if there are eight participants in all so that the private inputs are 7-dimensional hyperplanes, and one of the participants wishes to share his input with the others in such a way that a concurrence of any pair out of a particular subset of three of them or any concurrence of three participants will be able to act in his stead, it is difficult to see what the shares should be. It is easy to realize either a simple 2-out-of-3 or a 3-out-of-7 threshold scheme. In the first case, the shares could be three pairwise skew 3-spaces while in the second, the shares could be taken to be a pencil of 3-spaces chosen so that every pair intersect in a line and no three of which lie in a 6-dimensional subspace. The difficulty lies in constructing the three 3-spaces that are to be used for the shares for the three participants who are more trusted than the others so that they also function as shares in the 3-out-of-7 scheme. The only general solution we have found for problems of this sort, i.e., for trust schemes more complex than simple threshold schemes, makes use of the geometric dual to conventional shared secret schemes.

Points and hyperplanes are dual objects in any space. Conventional shared secret schemes are designed to conceal (and reveal) points, hence if we take the geometric dual of a conventional shared secret scheme replacing geometric unions by intersections and vice versa, we realize a scheme with the same control characteristics but in which the controlled object is a hyperplane instead of a point. Since the private pieces of information are points in the companion shared secret scheme, the private pieces of information will be hyperplanes in the dual scheme. We remark that while these dual constructions guarantee the existence of democratic shared secret schemes whenever shared secret schemes exist, the constructions that result may be unnecessarily complicated, as the examples will show.

While the discussion of shared secret schemes given here is purely geometric, there are other ways of looking at such schemes—which even if they prove to be equivalent may be very useful since they can draw on related disciplines in constructing such schemes. One of the more promising of these alternative formulations is based on the relationship between the reconstruction of a piece of information from partial information and the error correcting properties of error detecting and correcting codes, and in particular to maximum distance separable (MDS) codes.

The connection between shared secret schemes and Reed-Solomon codes has previously been observed by McEliece and Sarwate [3]. Reed-Solomon codes are special cases of Maximum Distance Separable Codes—MDS codes [2, Chapter 11]. These are block codes over some finite field GF(q) with block length n and q^k codewords. We will use the customary notation (n,k)-code. They have a property which is important in this context: the codeword can be reconstructed from any k of the n components of the codeword and if less than k components are known the remaining components are completely undecidable. Using the terminology of error correcting codes we say that the code is capable of correcting n-k erasures.

The use of MDS codes to construct autocratic secret shared schemes, i.e., with the assistance of a trusted authority, is straightforward: the authority randomly selects a codeword from an (n,k) MDS code. The selected codeword, or a part of it (say it's first component) may be regarded as the secret. Remaining components are distributed along with their position numbers in the codeword to the participants in the scheme. From the property of MDS codes described above it is clear that any k of the participants can reconstruct the codeword. A more general case, where some of the shares may be in error, is treated in [3].

In the absence of a mutually trusted party we modify this scheme to fit the protocol for setting up democratic shared control schemes described earlier. Each of the participants selects an (n,k) MDS code. Note that the choice of n and k may be different for each participant. Each participant then randomly selects a codeword in the code that he chose. These codewords are their shares in a unanimous consent scheme. The secret is the vector sum over GF(q) of their shares, which may require padding with trailing zeroes to obtain the same length.

Each participant now distributes distinct components, with position numbers, of his randomly selected codeword to a selected subset of the other participants whom he trusts to act in his stead. Due to the property of MDS codes any k (where k is the indicidual choice of the distributing particiapnt) of the members of the subset can reconstruct the participant's codeword.

In the simplest case of the above scheme a common (n,k) MDS code (where n is at least as large as the number, ℓ, of participants) is chosen beforehand. Each participant then, as his share in the unanimous consent scheme, randomly selects a codeword in the given code. In geometrical terms the shares are points on a k-dimensional hyperplane (through the origin) in the n-dimentional space over GF(q).

Each participant then distributes components and position numbers to all the other participants. Since the parameter k now is common to all the participants any k of them determine the shares of all the participants and thus the joint secret. We thus have realized a simple k-out-of-ℓ threshold scheme without the assistance of a mutually trusted party.

Examples

The smallest example that fully illustrates the protocol is a 2-out-of-3 threshold scheme. Such a scheme might be used to allow any two out of three vice-presidents at a bank to open the vault door but to insure that no one of them alone could do so. We will show how the three vice-presidents can set up such a scheme using either the point or plane protocol described above. In either case, the vault combination (the secret) can be thought of as a point in some suitable space.

For the first unanimous consent scheme the secret can be taken to be any point, p, on a line, say $\ell = PG(1,q)$. Each of the three participants secretly and randomly chooses a point, p_i, on ℓ. p is defined to be the field sum of the three points;

$$p = \sum_{i=1}^{3}\!\!\!\!\!\!\!\oplus\;\; p_i \quad . \qquad (1)$$

Clearly $\sum\!\!\!\!\!\!\oplus\;$ satisfies the definition of an entropy preserving sum, since as any single summand, p_i, ranges over all q+1 possible values, with the other two points remaining fixed, p also ranges over all of the points on the line.

The inescapable conclusion that follows from the acceptability of a 2-out-of-3 threshold scheme is that each participant is willing to trust the other two to only initiate the controlled action (i.e., to open the vault door in the present example) when they should. By the same token, the need for a 2-out-of-3 concurrance presupposes a lack of confidence in what a single individual might do. Consequently each participant (in this example) must logically be willing to share his private input to the secret between the other two participants in such a way that they could jointly reconstruct his contribution, but in which they are individually totally uncertain of it. To do this, each participant constructs a private 2-out-of-2 scheme of the sort described earlier, i.e., he randomly chooses a pair of points whose sum is his contribution to the democratic shared secret scheme, and gives (in secret) each of the other participants a different one of these points. A convenient way to represent this implementation of the protocol is:

$$\begin{array}{c|ccc|} & 1 & 2 & 3 \\ \hline 1 & p_1 & p_{21} & p_{31} \\ 2 & p_{12} & p_2 & p_{32} \\ 3 & p_{13} & p_{23} & p_3 \\ \hline \end{array}$$

where the three points in column i are all chosen by participant i— subject to the condition that $p_i = \sum_{j \neq i} p_{ij}$. The three entries in row j are known to participant j: the entry on the diagonal because he chose it and the off diagonal entries because they are the private pieces of information (points) given to him by the other participants. Clearly, any two participants have between them all the information needed to compute $p = \sum p_i$, while any one of them is totally uncertain as to the value of p. Although we have described the protocol starting with the establishment of the democratic unanimous consent scheme, the scheme would probably be implemented in reverse order. Participant i would choose at random the two points p_{ij}, $j \neq i$, and then calculate his input, p_i, to the unanimous consent scheme $p_i = \sum_{j \neq i} p_{ij}$, etc.

To set up the other type of unanimous consent scheme each participant chooses at random a plane, π_i, in a projective 3-space PG(3,q). As was noted earlier, since there are three participants, the second type of scheme is only possible in a 3-dimensional space. With virtual certainty (with increasing size of q), the three randomly and independently chosen planes intersect in only a single point. This point, p, is the jointly determined secret (combination) $p = \bigcap_{i=1}^{3} \pi_i$. This protocol defines a 3-out-of-3 unanimous concurrence scheme, since the three vice-presidents acting together can cause the secret to be reconstructed within the vault door mechanism at any time by reentering their private pieces of information (planes).

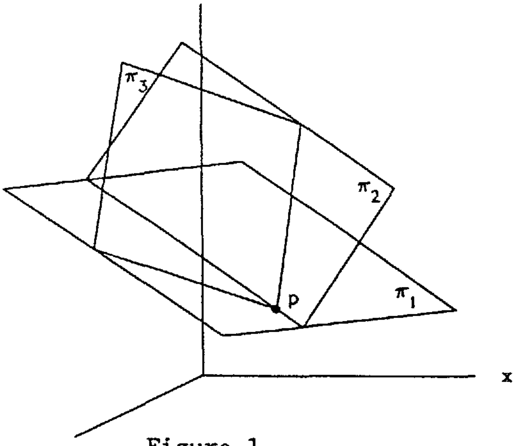

Figure 1.

As before, each participant also sets up a private 2-out-of-2 shared secret scheme to distribute information about the plane he chose to the other participants, constructed so that they can jointly reconstruct his plane, but individually cannot do so. One way he could do this would be to choose a pair of distinct lines lying in his plane and then give a different one of these lines to each of the other participants (in private). Since the lines are distinct, they span the plane. Hence any two vice-presidents have between them the capability to reconstruct all three planes and thus redefine p. The private pieces of information for each participant will be the plane he chose and the two lines given to him by the other vice-presidents. Since the pair of lines are shares in a perfect 2-out-of-2 scheme defining his secret plane, each vice-president is assured that a successful concurrence must either include him as a participant or else include both of the other vice-presidents. A convenient way to represent this implementation of the protocol is

$$\begin{array}{c|ccc|}
 & 1 & 2 & 3 \\
\hline
1 & \pi_1 & \ell_{21} & \ell_{31} \\
2 & \ell_{12} & \pi_2 & \ell_{32} \\
3 & \ell_{13} & \ell_{23} & \pi_3 \\
\hline
\end{array}$$

where the lines (off diagonal) entries in column i are chosen by participant i—subject to the condition that they span the plane π_i, $\pi_i = \bigcup_{j\neq i} \ell_{ij}$. The three entries in row j are known to participant j: the entry on the diagonal because it is the plane he chose and the off diagonal entries because they are the private pieces of information (lines) given to him by the other participants.

This construction—for distributing shares of the participant's private inputs—does not use the geometric dual of a companion shared secret scheme. If we wish to use this technique, we must work in the full 3-space since the dual of a point must be plane: the participant's input which he wishes to share with the other participants. Consequently, the companion shared secret scheme would have to be of the form shown in Figure 2.

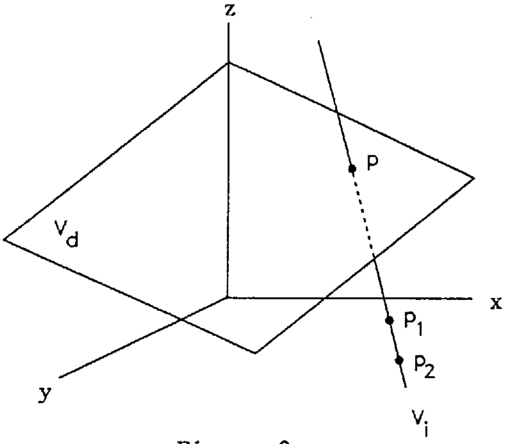

Figure 2.

The union (span) of the two points p_1 and p_2 (the shares of the point p in this scheme) is the line V_i which intersects the publicly known plane V_d in the (secret) point p. In the dual construction, Figure 3,

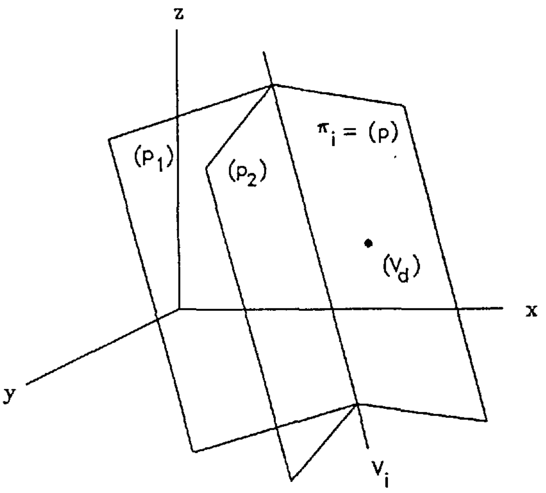

Figure 3.

the intersection of the two planes (p_1) and (p_2) (the shares of the plane (p) in the dual scheme) is the line V_i whose union with the publicly known point (V_d) is the secret plane (p). In other words, to use a dual shared secret scheme to share a plane, π_i, each participant would make public a point, (V_d), in the plane and then give to each of the other participants one out of a pair of planes whose intersection is a line, V_i, in π_i but not on the publicly known point (V_d). Clearly, this is an alternative construction to the one described first for a democratic 2-out-of-3 shared secret scheme, but equally clearly, not as efficient. Each participant's private information now consists of three planes: the one he chose and two given to him by the other participants. In addition, there are three publicly known points that are essential to the shared secret scheme.

In view of the complexity of the dual geometric construction just given, one might question whether the technique has any application. We conclude by exhibiting an example in which (so far as we have been able to determine) it is the only means of constructing a solution. We mentioned earlier a shared secret scheme in which a participant is willing to trust any three of the other participants or any pair out of a specified subset of them to represent his interests. While it is easy to realize efficient k-out-of-ℓ threshold schemes in general, it is very difficult to realize schemes in which the members of one class can function as members of another (less capable) class. Simmons [5,7] has discussed multilevel shared secret schemes of this sort and shown how to solve them in general—where the secret information is a point in some space. Figure 4 shows a construction for a two-level control scheme satisfying the controls just described.

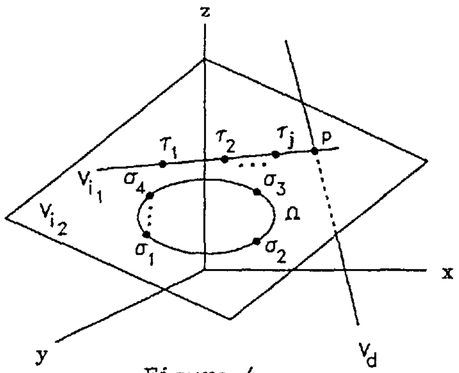

Figure 4.

The secret is the point, p, on the line V_d at which both the plane V_{i_2} and the line V_{i_1} (in the plane) intersect it. The private pieces of information held by the more capable class (the 2-out-of-ℓ_2 shared control scheme) are points τ_i one the line V_{i_1}; $\tau_i \neq p$. The private pieces of information held by the less capable class (the 3-out-of-ℓ_3 shared control scheme) are points σ_i on the oval Ω, where the points σ_i and τ_i are chosen so that no pair of the points on Ω (used as private pieces of information) are collinear with a point τ_i or with p on the line V_{i_1}.

The dual construction to this scheme is shown in Figure 5.

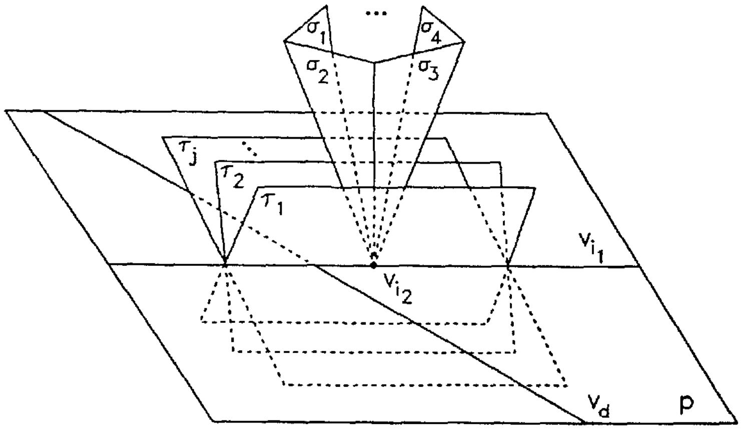

Figure 5.

The set of points σ_i on Ω, in Figure 4 no three of which are collinear and no pair of which are collinear with a point r_i on V_{i_1} (or with p), have been replaced in Figure 5 by the sheaf of planes π_i on the point V_{i_2} (dual to the plane V_{i_2} in Figure 4) no three of which intersect in a common line and none of which contain the line V_{i_1}. Similarly, the set of collinear points r_i on the line V_i in Figure 4 have been replaced by a pencil of planes on a common line V_{i_1} in Figure 5. The dual of the point p lying on the line V_d (and on the plane V_{i_2} and the line V_{i_1}) in Figure 4 is the plane p containing the point V_{i_2} and the line V_{i_1} in Figure 5. It is an easy matter to show that this dual configuration has the desired control characteristics. The line V_d (a unique line for each participant who wished to implement this sort of sharing of his secret input with the other participants) would be made public. Each participant would be (privately) given a plane as his share of the input. While it might be possible to devise a way of giving only lines and points in a plane as shares to the other participants to realize such a two-level control scheme, we have been unable to find such a construction. The directness of the geometric dual constructions may more than compensate for their lack of efficiency even if alternative constructions exist—which appears very doubtful for complex control schemes.

Conclusion

The protocol described here is so simple in principal that there is no question about its feasibility in practice—even though the private shared secret schemes may themselves require complex implementations to realize desired concurrences. The essential point is that the protocol insures that no participant can increase his capability (to contribute to the reconstruction of the secret) beyond what is acceptable to the other participants. However, an extended protocol is required if one also wishes to insure that a participant can't diminish the capability of other participants as well; i.e., to cause concurrences whose members believe they have the capability to recover the secret to not be able to do so. The authors plan to treat these extended (capability) protocols in a subsequent paper.

The bottom line is that the protocol described here permits democratic shared secret schemes, which must logically be trusted, to be set up by mutually distrustful parties without outside assistance. In addition, no participant is required to accept a greater risk of the secret information being misused than what he would have had to be willing to accept if there had existed a trusted authority to set up the scheme instead. Clearly this is the most that could be hoped for.

References

1. I. Ingemarsson and G. J. Simmons, "How Mutually Distrustful Parties Can Set Up a Mutually Trusted Shared Secret Scheme," International Association for Cryptologic Research (IACR) Newsletter, Vol. 7, No. 1, January 1990, pp. 4-7.

2. F. J. MacWilliams and N.J.A. Sloane, "The Theory of Error Correcting Codes," North Holland, Amsterdam, 1981.

3. R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," Communications of the ACM, Vol. 24, No. 9, Sept. 1981, pp. 583-584.

4. C. Meadows, "Some Threshold Schemes Without Central Key Distributors," Congressus Numerantium, 46, 1985, pp. 187-199.

5. G. J. Simmons, "How to (Really) Share a Secret," Crypto'88, Santa Barbara, CA, August 21-25, 1988, Advances in Cryptology, Vol. 403, Springer-Verlag, 1989, pp. 390-448.

6. G. J. Simmons, "Robust Shared Secret Schemes or 'How to be Sure You Have the Right Answer Even Though You Don't Know the Question'," 18th Annual Conference on Numerical Mathematics and Computing, Sept. 29-Oct. 1, 1988, Winnipeg, Manitoba, Canada, Congressus Numerantium, Vol. 68, May 1989, pp. 215-248.

7. G. J. Simmons, "Prepositioned Shared Secret and/or Shared Control Schemes," Eurocrypt'89, Houthalen, Belgium, April 11-13, 1989, Advances in Cryptology, to appear.